

**State of Arizona**  
**PLAN REVIEW AND VALIDATION, PHASE II**  
**APRIL 2005 – OCTOBER 2005**



**BUSINESS  
CONTINUITY  
PLANNING GUIDE**

An all-hazards, functional approach to Business Continuity Planning, preparedness, emergency response and recovery activity for State Agencies, Boards and Commissions.

PREPARED BY:

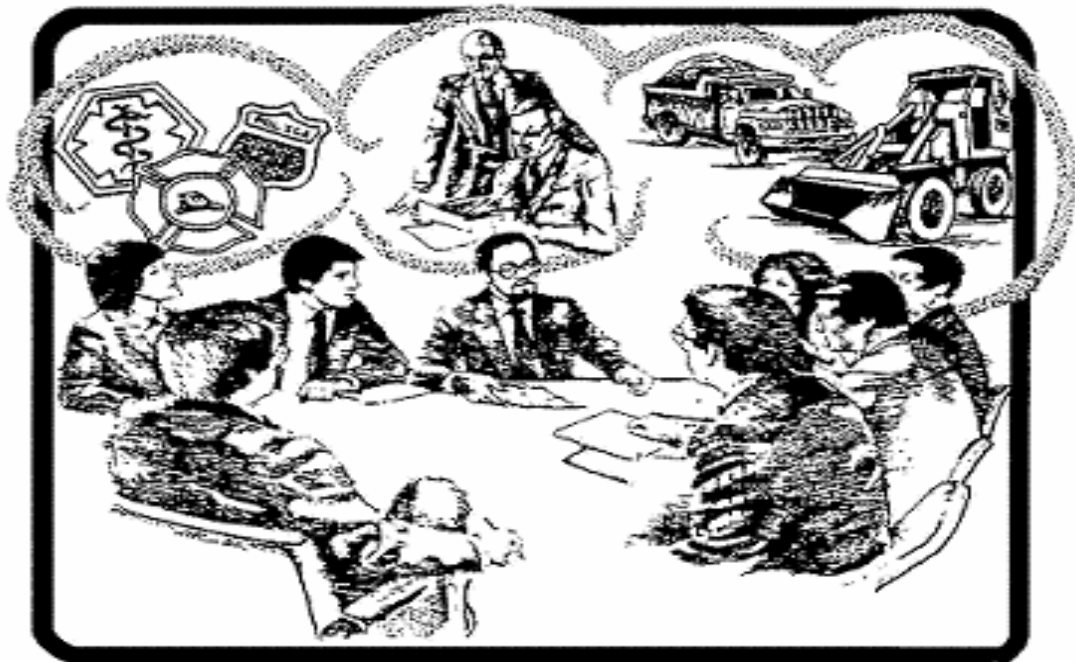
**DEPARTMENT OF EMERGENCY & MILITARY AFFAIRS**  
**ARIZONA DEPARTMENT OF ADMINISTRATION ♦ GOVERNMENT INFORMATION TECHNOLOGY AGENCY**

## Table of Contents

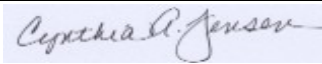
<b>INTRODUCTION .....</b>	<b>IV</b>
<b>PLAN REVIEW AND VALIDATION PROCESS .....</b>	<b>1</b>
CALENDAR YEAR 2005 PLAN DELIVERABLES AND TIMEFRAME TABLE .....	1
PHASE 2 PROGRAM SCOPE .....	2
SUBMISSION REQUIREMENT: .....	2
<b>OVERVIEW .....</b>	<b>3</b>
BUSINESS CONTINUITY PLANNING IN STATE AGENCIES .....	3
RELATIONSHIP BETWEEN STATE PLAN DOCUMENTS .....	4
INTER AND INTRA AGENCY COMMUNICATION RELATIONSHIPS .....	5
SPECTRUM OF ACTIVITY .....	5
CONTINUUM FOR BUSINESS CONTINUITY PLANNING .....	6
<b>GETTING STARTED – PROJECT INITIATION AND MANAGEMENT .....</b>	<b>7</b>
ESTABLISH A BUSINESS CONTINUITY PLANNING TEAM .....	7
CREATE A PROJECT PLAN – STEP 1 .....	8
ASSESS CURRENT BUSINESS CONTINUITY PLAN STATUS - STEP 2 .....	8
DISASTER RECOVERY PLANNING (DRP) FOR IT .....	9
PLAN REVISION OUTLINE – STEP 3 .....	11
PROJECT COMPARISON WORKSHEET .....	12
PLANNING AND PREPARATION .....	13
<b>THREAT ANALYSIS .....</b>	<b>16</b>
THREAT IDENTIFICATION .....	16
PROPERTY PROTECTION .....	16
<b>EMERGENCY COORDINATION .....</b>	<b>17</b>
COORDINATE WITH EMERGENCY SERVICE PROVIDERS AND STAKEHOLDERS .....	17
EMERGENCY PROCEDURES .....	18
<b>INCIDENT MANAGEMENT .....</b>	<b>20</b>
<b>INCIDENT MANAGEMENT .....</b>	<b>21</b>
PLAN ACTIVATION .....	21
COMMUNICATION .....	21
ADMINISTRATION AND LOGISTICS .....	21
INCIDENT COMMAND .....	22
AFTER ACTION REPORTS .....	22
<b>BUSINESS CONTINUITY AND RECOVERY .....</b>	<b>23</b>
DAMAGE ASSESSMENT .....	23
SALVAGE AND RESTORATION .....	23
BUSINESS PROCESSES .....	23
RETURN TO NORMAL OPERATIONS .....	24
COMMUNICATION .....	24
<b>TRAINING PLAN .....</b>	<b>25</b>
EMPLOYEE ORIENTATION AND TRAINING .....	25
<b>EXERCISE AND REVISE .....</b>	<b>27</b>
TABLETOP EXERCISE .....	27
FUNCTIONAL EXERCISE .....	28

## PHASE II

<b>MAINTENANCE AND CONTINUOUS IMPROVEMENT PLAN .....</b>	<b>29</b>
OPERATIONAL INTEGRATION .....	29
ANNUAL PLAN UPDATES AND AUDIT .....	29
COMPLIANCE .....	30
<b>APPENDIX A:.....</b>	<b>31</b>
TRIGGER/RESPONSE FLOW CHART .....	31
<b>APPENDIX B:.....</b>	<b>32</b>
POLICY MANAGEMENT TEAM.....	32
<b>APPENDIX C:.....</b>	<b>33</b>
PROPOSED TEAM STRUCTURE.....	33
<b>APPENDIX D:.....</b>	<b>34</b>
DISASTER RECOVERY PLANNING (DRP) FOR IT .....	34
<b>APPENDIX E .....</b>	<b>38</b>
TASK TRAINING OUTLINE.....	39
<b>APPENDIX F: .....</b>	<b>40</b>
SAFEGUARDING (FOR OFFICIAL USE ONLY) INFORMATION.....	40
<b>ACRONYMS.....</b>	<b>48</b>
<b>GLOSSARY .....</b>	<b>51</b>



**State of Arizona**  
**BUSINESS CONTINUITY PLANNING GUIDE**  
**RECORD OF CHANGES**

Change Number	Change Date	Date Entered	Change Made By (Signature)
Initial Release		4/6/05	
Revised Pg. 9	7/12/05	7/12/05	

### INTRODUCTION

Every year emergencies and disaster conditions take their toll, indiscriminately in both the public and private sector, throughout the United States. Arizona has experienced these conditions in the past and will again in the future. Flooding has caused significant problems in the state along with wildland fires and hazardous materials incidents. Unstable world conditions, natural and technological disasters will continue to affect our expanding population in Arizona. State agencies can limit injuries to their staff, protect the public in and around their facilities, reduce property damage and quickly return to work with an effective **Business Continuity Plan**. The State of Arizona, **Emergency Response and Recovery Plan**, was designed to accomplish a similar level of support for counties and cities.

This Guide (Phase II) provides recommendations on how to review, update and maintain your agency's comprehensive Business Continuity Plan and preparedness program to allow the critical business of government and supporting information technologies to continue during emergencies. Mid-year 2003 Arizona State Agencies, Boards and Commissions submitted their Business Continuity Plans to the Department of Administration for review by a task force from ADOA, GITA and DEMA, pursuant to the Governor's Executive Order #2003-05, dated January 13, 2003. A summary report was sent to the Governor on September 2, 2003 outlining the readiness positions and advances state agencies, boards and commissions have made in preparing their Business Continuity Plans. Major strides were made in upgrading agency plans, training staff and completing preparedness exercises.

Previously, Phase I (2002-2003), called for the development of agency Business Continuity Plans utilizing a software template or related outline. This year Phase II, (2005) emphasizes plan review, validation and updating of existing Business Continuity Plans. Strategic direction in the BCP development process includes Phase III (2006), which will stress the interdependency of agencies supporting the resumption of critical business functions and supporting information technologies. Future plans also call for:

1. Planning initiatives utilizing an electronic format that will enable secure access to agency plans with additional storage capability offsite,
2. Cost accounting for time and materials to quantify the cost of disasters, and
3. The use of the Internet and Intranet are being surveyed to provide optimum use, with the ability to access and manipulate data quickly.

Input from the agencies will continually be sought concerning format and design for future BCP models, evaluation and the testing of applications. Your input will be very much appreciated.

The goal for Phase II of development is to refine, expand and validate the capability outlined in your agency's existing Business Continuity Plan (BCP). Business Continuity Plans should be dynamic documents that can be easily manipulated

## PHASE II

electronically and capable of fully meeting the needs of the staff in the restoration and recovery of critical business activities for your agency for up to one month.

Your plan should assist your organization to prepare for, mitigate, respond to and recover from a business and/or cyber disruption. The diagram in the upper right hand corner of the text represents the phase in the development of your plan.

This planning guidance was not developed to ensure compliance with any specific federal, state, or local codes statute or administrative rule that may apply to one or more of your facilities. Specific requirements should be addressed by contacting appropriate agencies such as:

- Occupational Safety and Health Administration (OSHA),
- US Environmental Protection Agency (EPA),
- US Department of Treasury,
- US Department of Human and Health Services,
- US Department of Justice,
- Governor's office,
- Arizona Criminal Justice System,
- Arizona Department of Administration.
- Government Information Technology Agency (GITA)

Individual, unit and collective training, conducting drills and exercises, testing systems and equipment and coordinating with local emergency services providers are all important functions in this phase. Use the steps provided in "Getting Started – Project Initiation and Management" to initiate your review process. Thank you for your assistance in contributing to this effort, which collectively will provide a valuable service to the State of Arizona, your fellow staff members and the public we serve.

**David P. Rataczak**  
Major General, AZ ARNG  
The Adjutant General  
Department of Emergency  
and Military Affairs (DEMA)

**Ms. Betsey Bayless**  
Director,  
Arizona Department of  
Administration

**Mr. Chris Cummiskey**  
Director,  
Government Information  
Technology Agency

### Acknowledgements

Acknowledgement is given to the following individuals and their organizations for their support in the development of this Phase II guidance document and programs.

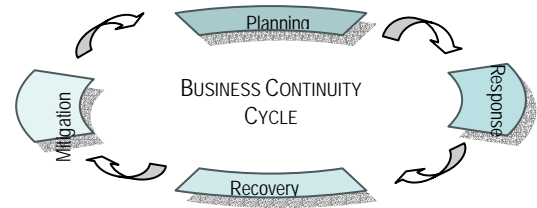
**Mr. John W. Paulsen**  
Manager,  
Homeland Security  
Planning, DEMA  
602-231-6224

**Mr. Lee Lane**  
Statewide Security Manager  
Dept. of Administration  
(602) 542 – 2302

**Mr. James M. Ryan**  
Homeland Security Manager  
Government Information  
Technology Agency  
(602) 364 – 4771

**Ms. Cynthia Jensen**  
Business Continuity  
Planner,  
DEMA  
602-231-6204

March 1, 2005



## PLAN REVIEW AND VALIDATION PROCESS

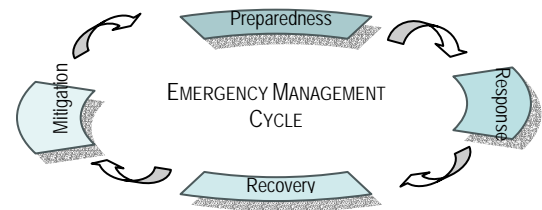
Several planning deliverables are involved in the assessment, planning and revision of your current Business Continuity Plan. Plans are based upon efforts within an agency to assure that capability exists to provide critical services across a wide range of potential hazards. Plans should utilize a comprehensive, all-hazards approach to address essential government functions. The process consists of a continuing cycle of **preparedness planning, training and exercise** activity for your agency. Utilize the following timeline under each area listed below to complete the development of your revised Business Continuity Plan:

### Calendar Year 2005 Plan Deliverables and Timeframe Table

Establish an internal agency schedule with milestones to guide the project to completion no later than October 31, 2005.

Date	Work Products	Action / Deliverables
<b><u>Planning</u></b>		
<b>April:</b>	Appoint Emergency Services Program Coordinator (ESPC) Form an Emergency Planning Team Create Project Plan	Return Appointment Form by April 30, 2005
<b>May:</b>	Assess Agency Business Continuity Plan ESPC Attend Project Orientation Session	Return Registration Form
<b>June:</b>	Initiate Plan Revision Outline Attend BCP Development Workshop	Submit Project Plan Return Registration Form
<b><u>Training</u></b>		
<b>June/July:</b>	Employee Plan Orientation and Staff Development/Training	
<b><u>Exercise</u></b>		
<b>Aug/Sept:</b>	Conduct Tabletop Exercise	Submit After Action Report
<b>Sept:</b>	Revise Agency Plan	Produce and Distribute Plan
<b>October:</b>	Agency Plan Briefing for staff	<b>Submit Revised Plan October 31, 2005</b>

## PHASE II



The Arizona Department of Emergency and Military Affairs (DEMA), the Arizona Department of Administration (ADOA) and the Government Information and Technology Agency (GITA) produced this guidance. For comments, questions or information about this document, agency planning initiatives or the state *Business Continuity Planning Program* and support initiatives please contact Ms. Cynthia Jensen, DEMA, Business Continuity Planner at (602) 231-6204 or azbcp@azdema.gov.

### Phase 2 Program Scope

#### Step 1: The Business Continuity Planning Team/Emergency Program Coordinator

- Energize your planning team

#### Step 2: Assess the status of your Business Continuity Plan

- Accomplish an agency strategic and tactical review

#### Step 3: Revise your plan

- First /Second Draft

#### Step 4: Staff Development

- Establish schedule, orient and train your staff

#### Step 5: Exercise your plan

- Tabletop exercise

#### Step 6: Update your plan

- Final draft

#### Step 7: Implement your plan

- Operational integration and plan maintenance
- Submission Requirement

#### Step 8: Activate your plan

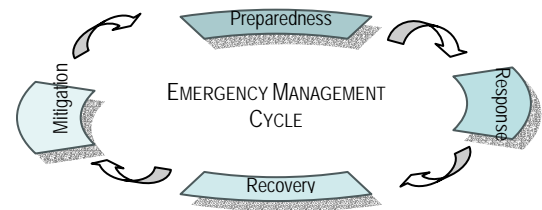
- After Action “Lessons Learned” Reports

### Submission Requirement:

Submit your revised Business Continuity Plan in hard copy form and on a CD for evaluation and review, no later than October 31, 2005 to the following address:

Ms. Cynthia Jensen  
Business Continuity Planner  
Arizona Division of Emergency Management  
5636 E. McDowell Road  
Phoenix, Arizona 85008





## OVERVIEW

### Business Continuity Planning in State Agencies

Whether you operate from the Capitol Mall or remote area; represent a large or small agency, the concepts in this guide will maintain universal application. The most significant aspect of the program remains the support provided by your chief executive officer and your management structure to make business continuity planning and preparedness a priority initiative in your organizational culture. The magnitude of an emergency or disaster is relative to the size of the organization and the impact of the natural or technological event. What might constitute a disaster for a small facility may in fact be only a nuisance to a larger agency or facility.

An emergency is an unscheduled event that can cause significant injuries to employees or the public or disrupt normal business operations and damage the environment. These events may be the result of natural, technological, or human caused conditions. Business continuity **planning** is a dynamic process developed to prepare for, mitigate, respond to and recover from a disruptive event. Business continuity planning, although critical is one of several vital components. **Training**, conducting drills and **exercises**, testing equipment and coordinating with community emergency services providers are other critical preparedness functions.

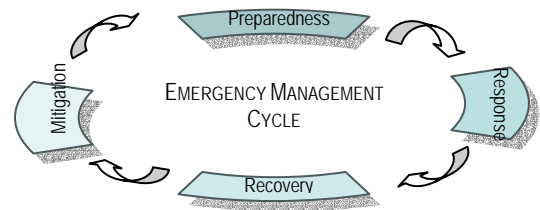
#### The “case” for Business Continuity Planning

- During a service interruption, the agency business services continue to the public,
- Facilitates compliance with federal, state and local statutes and administrative rules,
- Reduces exposure to civil or criminal liability in the event of an incident by maintaining the “standard of care,”

**Disclaimer:**

*Inclusions of references to vendor concepts or methods in these guidelines are for information purposes only. The appearance or absence of a vendor or product in this publication should not be construed as an endorsement or non-endorsement of a specific vendor, product, service or company.*

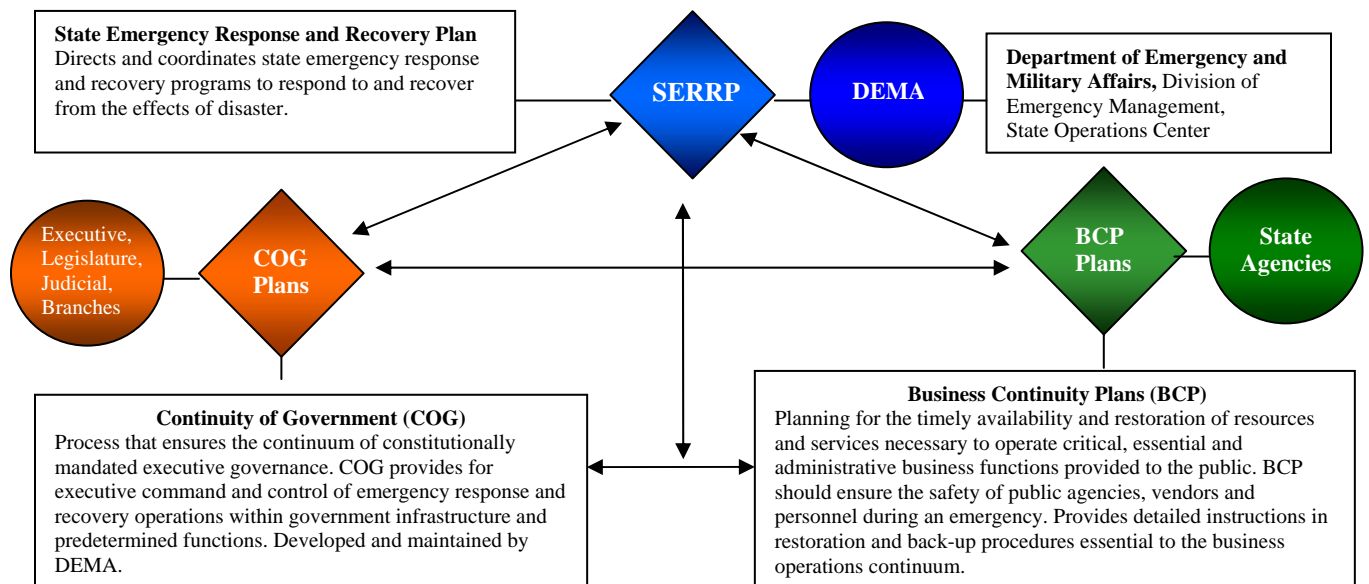
*Published and distributed by the Department of Emergency and Military Affairs. April 2005*

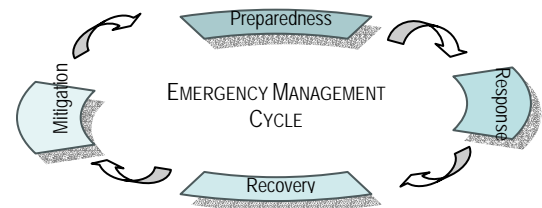


## Relationship Between State Plan Documents

Contingency Planning is a critical part of the emergency preparedness initiatives developed by the State of Arizona to enable government agencies to reduce the potential impact of natural and technological disasters on routine operations. The following diagram illustrates the relationship of the various emergency plans to one another and their individual function.

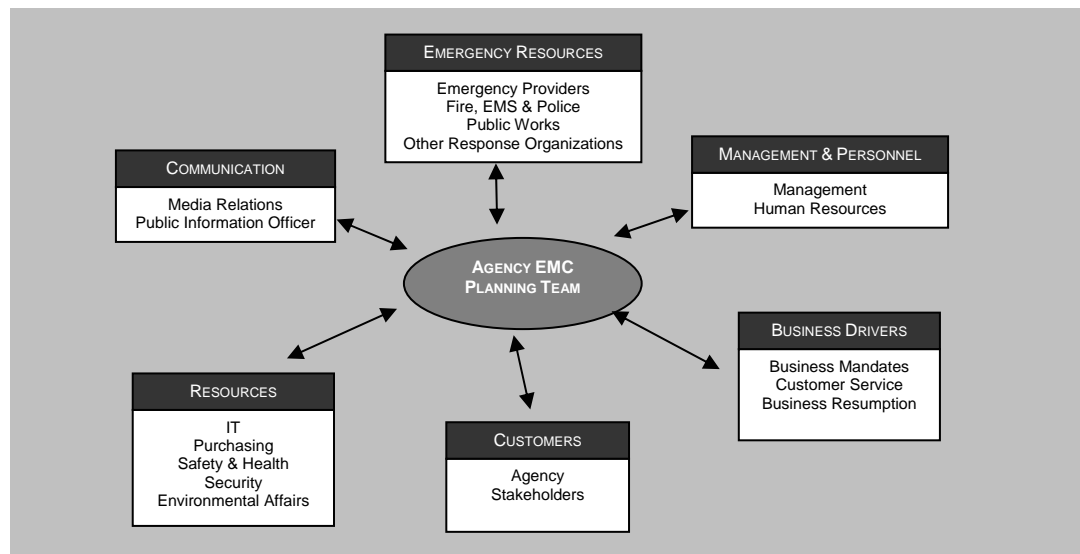
**Relationship Between State Plan Documents**  
Relationship Diagram





## Inter and Intra Agency Communication Relationships

The diagram below outlines the relationships and communications flow between the planning team, management, support services, community agencies and emergency services providers and stakeholders.



## Spectrum of Activity

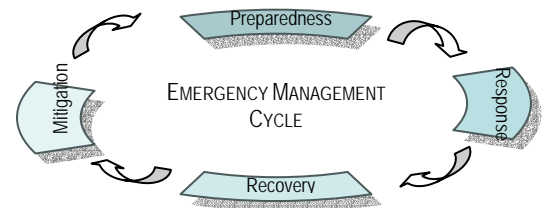
The following diagram represents a broad spectrum of activities that are all part of a structured business continuity program. The diagram is divided into three parts to illustrate institutional activity prior to, during and after a disaster.

**Before the disaster** strikes is the appropriate time to prepare an organization for the adverse affects of a natural or technological event that could directly impact continuing operations. Preparing a Business Continuity Plan and training staff will help achieve this objective. Control of emergency functions should take place at an agencies control point, their Operations Center, either a fixed or mobile site.

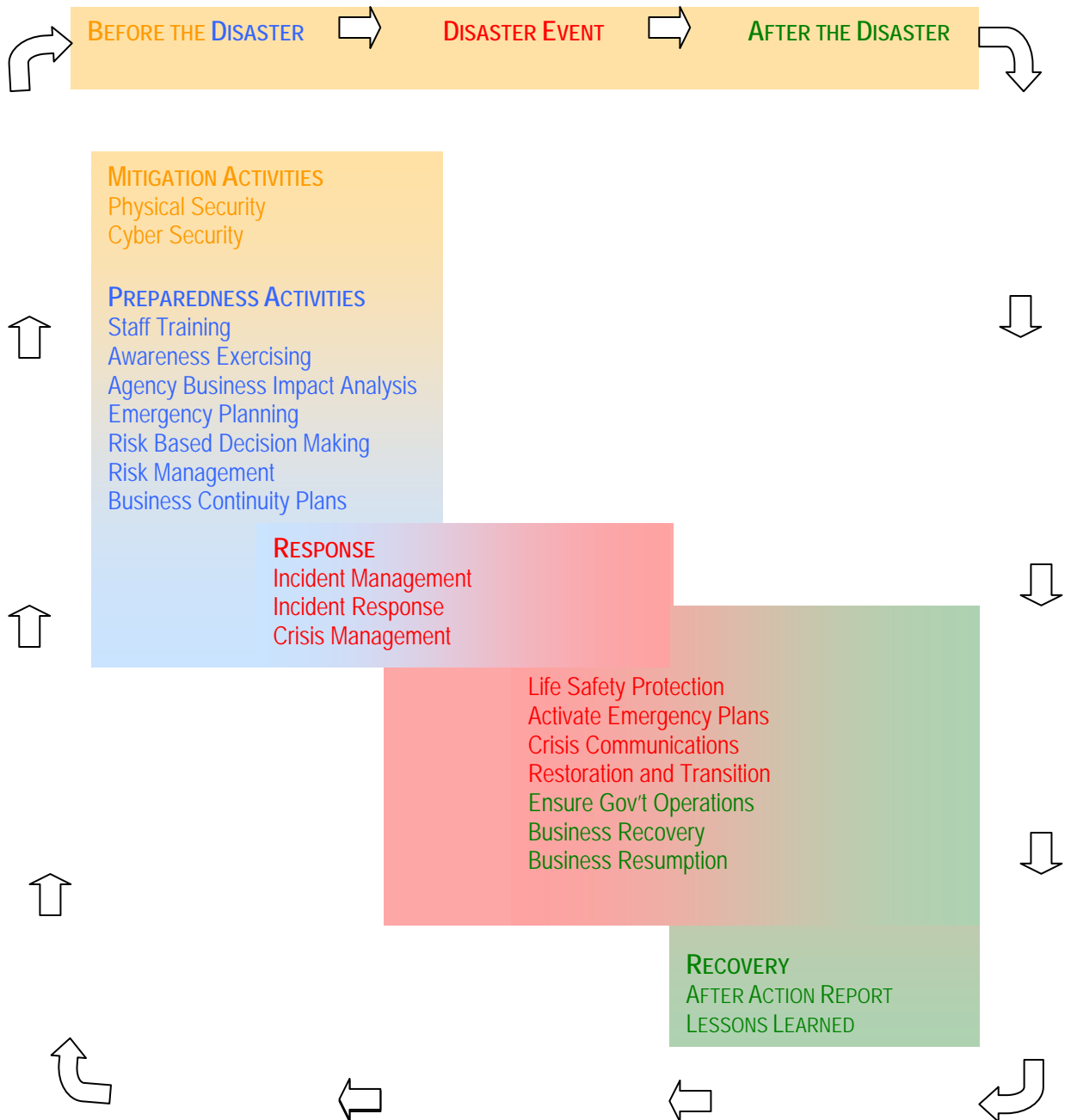
**Disaster Events** depicts an array of emergency response and life safety actions, available to decision makers, which can be taken to preserve and protect the public and the organizational structure of the agency.

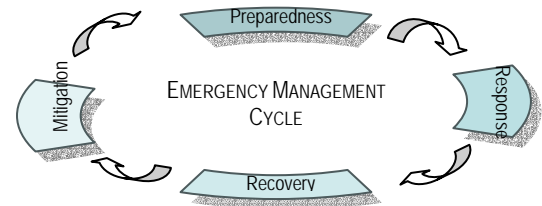
**After the disaster** response operations merge into recovery programs and the restoration of critical business functions are completed. Explore mitigation possibilities to avoid future occurrences. Consider both “*structural*” mitigation, (protecting equipment from future losses) and “*non-structural*” mitigation (which would include planning initiatives such as updating codes or zoning requirements).

## PHASE II



## Continuum for Business Continuity Planning





## GETTING STARTED – PROJECT INITIATION AND MANAGEMENT

### Establish a Business Continuity Planning Team

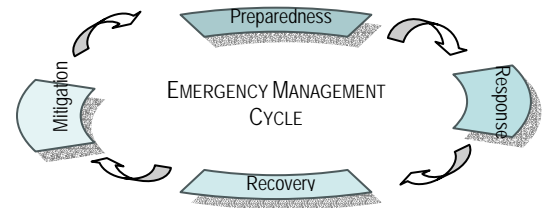
Form an emergency planning team and appoint members to support and direct the development of your revised Business Continuity Plan. The size of the team will depend upon agency structure and the available resources of your organization. An Emergency Services Coordinator (ESC) should be appointed to manage the planning process and serve as a point of contact for the agency director. A mid-level manager with a good understanding of the total organizational culture would make a good choice to act upon the behalf of the director. One or two members of the team will probably complete most of the development work with others serving in a review and/or advisory capacity. An information specialist would make a good team member. Obtain input from all functional business units of the organization. Participants should be appointed in writing.

Participants do not need an in-depth knowledge of the emergency planning field, but they do need a good understanding of agency functions. The chief executive or senior manager should energize and direct the group while providing budget support. Staff job descriptions should reflect this critical task as an additional duty assignment.

#### ***Model duty description for an Emergency Services Program Coordinator***

*The incumbent has received an additional duty assignment as the agency, Emergency Services Coordinator (ESC). Primary duties will focus on the development of agency Business Continuity Planning according to the criteria established by the state. The ESC will successfully coordinate the development of the annual revision to the agency plan, attend orientation and training sessions and participate in other related support activity.*

*According to the Governors Executive Order 2004-05 posted in the State Emergency Response and Recovery Plan (SERRP) “Each state agency shall appoint an emergency coordinator and an alternate to act on behalf of the agency during an emergency or disaster, and shall furnish the name and contact telephone numbers to the Director of the Arizona Division of Emergency Management.”*



### Create a Project Plan – Step 1

Using the deliverables outlined in the Phase II Guidance, review this document and establish a project schedule and milestones for guiding the project to completion no later than October 31, 2005.

1. Create timelines and maintain a robust work schedule for reviewing and producing a new plan.
2. Create a mission statement for the project to define the task and structure the planning team.
3. Assign members of the planning team to draft revised portions of the plan based on a schedule, milestones and goals.
4. Utilize the Phase 1 template and add to your original plan.
5. Identify challenges, tasks to perform and prioritize activities.
6. Maintain a list of problem areas to address and resource shortfalls<sup>1</sup>.
7. Distribute the first draft for staff review.
8. Revise and negotiate as necessary.

The plan should be developed using concise language in a direct and easy to read style. A plan, excluding annexes should be no more than 100 pages in length or less and evaluated annually.

#### ***Model Mission Statement***

*Business Continuity Plans (BCP) shall be maintained by the Agency's leadership to support the operation of critical business functions during periods of natural, technological or human-caused disasters. An all-hazard approach to preparedness will be utilized to enhance agency capability to respond to and recover from potential business disruptions. Public health and safety will remain our primary responsibility along with the protection and preservation of property and the conservation of resources. BCPs will be reviewed annually and updated to reflect critical changes to agency personnel, facilities and resources including changes to mandatory services. Agency staff will receive preparedness orientations, training and participate in BCP drills and exercises.*

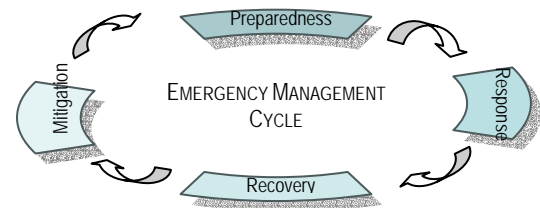
### Assess Current Business Continuity Plan Status - Step 2

Review your agency's current Business Continuity Plan, policies and procedures and supporting documentation.

---

<sup>1</sup> Note: You may want to "test" some of your problem areas in multiple tabletop exercises.

## PHASE II



- Does your emergency strategy accomplish what is required to be able to respond to, and recover from a business disruption?
- Are agency personnel tactically proficient in completing the tasks assigned them in your plan?

The following agency plans, related policies and procedures as well as specific agency reference materials may be helpful in your organizational review and should remain in your BCP file or accessible<sup>2</sup> as appendixes:

- Agency Legal Documents
- Agency Vulnerability Assessment
- Arizona State Revised Statutes
- Business Impact Study
- Employee Emergency Procedures
- Energy Plan
- Environmental Policy and Procedures
- Evacuation Plan, Routes and Procedure Procedures
- Hazardous Materials Plan
- Agency IT Plan (ITP)
- Technical Infrastructure & Security Assessment (TISA)
- Information Services Inventory System (ISIS)
- Protection of Public Documents
- Risk Management Plan
- Security Plan and Procedures
- Staff Notification Procedures
- Statewide Strategic IT Plan
- Finance and Procurement
- Management Succession Plan
- Fire Protection Plan
- Network/Systems Diagrams

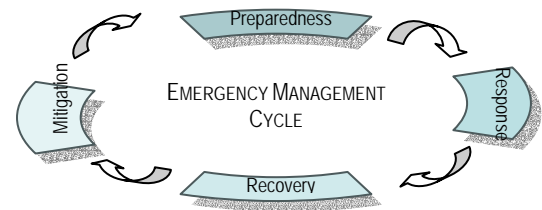
### Disaster Recovery Planning (DRP) For IT

The State of Arizona's Enterprise Architecture (EA) Governance is comprised of the Government Information Technology Agency (GITA), Arizona's CIO Council, and the Information Technology Authorization Committee (ITAC) that provides the leadership and development of statewide IT policies and standards for infrastructure and security schemes to promote the state's economy and public welfare.

---

<sup>2</sup> Accessible – Is defined as photocopied and attached to the BCP, or documenting where one might find a copy of the noted document, plan or Standard Operating Procedure document (SOP).

## PHASE II

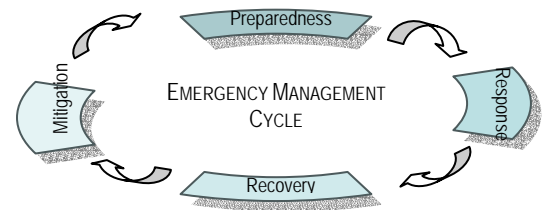


Therefore, Business Continuity Planning (BCP) in conjunction with Disaster Recovery Planning (DRP) for IT provides instruction, recommendations, and considerations for state government and IT to operate effectively without excessive interruption. DRP refers to interim measures to recover IT services following a business/program/agency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT function using manual methods.

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outages, disk drive failures) to severe (e.g. equipment destruction, fire) from a variety of sources such as natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the agency's risk management effort, it is virtually impossible to completely eliminate all risks. In many cases, critical resources may reside outside the agency's control (such as electric power and telecommunications) and the agency may be unable to ensure their availability. Thus effective DRP planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

The BCP and additional recommendations for DRP listed in Appendix-D of this guideline will provide preventive controls, recovery strategies, and suggested recovery teams common to all IT systems.





## Plan Revision Outline – Step 3

You are ready to revise your BCP. Your plan should include the following sections:

### SAMPLE PLAN OUTLINE

#### Introduction

The Introduction provides instructions for use of the plan, executive summary, and related documents. These elements should contain:

- A. Table of Contents
- B. Instructions for Use
- C. Record of Changes
- D. Executive summary

#### Basic Plan

The Basic Plan outlines, in narrative form, the purpose of the plan, authorities and the responsibilities of the agency to prepare for, respond to and recover from an emergency or disaster condition. An executive summary will provide management policies and a brief overview of the plan:

##### *1-Agency Identification*

- A. The purpose of the plan
- B. The agencies business continuity vision and policy
- C. Authority and responsibility of key staff positions, lines of succession
- D. Types of hazardous conditions that could arise
- E. Locations and description of the agency's operations center

Refer to Appendix A for flow chart depicting activation triggers and when they occur in the response flow process.

#### Functional Annexes

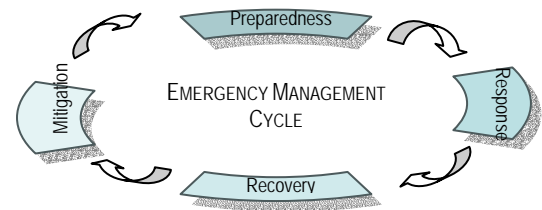
Functional annexes outline the responsibilities of departments, staff functions and support provided by state and local emergency providers in their response to and recovery from disasters. Annexes to your plan are like chapters in a book. Your current plan should include:

##### *2 - Summary of Areas of Responsibility*

##### *3 - Summary of Business Processes*

Additional annexes may be developed to address agency site-specific issues at your facilities.

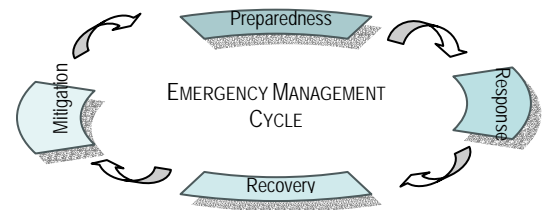
Numbered items in italics represent the planning templates from the previous 2003 Business Continuity Planning project. Use the format you created if you elected not to use the template or an alternate design. Template software remains available for your use at [www.security.state.az/business-continuity-planning.htm](http://www.security.state.az/business-continuity-planning.htm)



## Project Comparison Worksheet

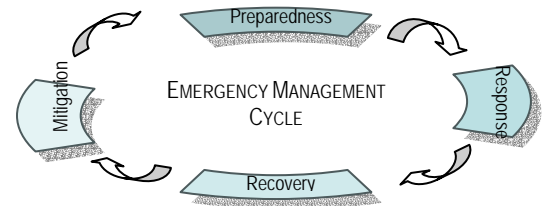
The planning model provided in our previous guidance included the elements located in the column on the left. Expanded program criteria are included in the center column. Your new plan should combine elements from both columns. See Step 3 of the Sample Plan Outline for additional information.

BCP TEMPLATE INFORMATION SUBMITTED IN 2003 (Your Current plan)	NEW ADDITIONAL PLAN REQUIREMENTS (See Planning Guidance)	AGENCY UPDATED PLAN (Due October 31, 2005)
		Title Page
	Introduction	Introduction
	Basic Plan	Basic Plan
Agency Identification	→	Agency Identification
	Functional Annexes	Functional Annexes
Summary of Areas of Responsibility	→	Summary of Areas of Responsibility
Summary of Business Processes	→	Summary of Business Process
Business Process Information	→	Business Process Information
Business Information and Documents	→	Business Information and Documents
Process Tasks	→	Process Tasks
Process Call Tree	→	Process Call Tree
Internal Agency Dependencies	→	Internal Agency Dependencies
External Dependencies	→	External Dependencies
External Contracts	→	External Contracts
Customer Contacts	→	Customer Contacts
Response/Recovery Team Personnel	→	Response/Recovery Team Personnel
Business Equipment And Supplies	→	Business Equipment and Supplies
Information Tech Applications	→	Information Tech Applications
Information Tech Server/Hardware	→	Information Tech Server/Hardware
Telecommunications	→	Telecommunications
Alternate Sites	→	Alternate Sites
	Agency Recovery	Agency Recovery

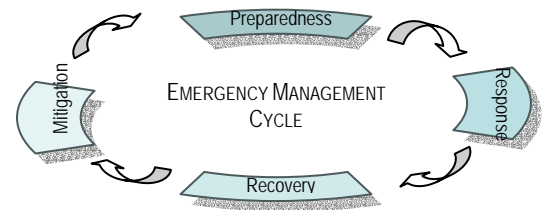


## Project Checklist

Your agency BCP should contain the following elements or address the items indicated. If your plan meets the outcome listed, place a check in the box to the right.	
<b>a) Personnel</b>	
i) Has an Emergency Services Program Coordinator been appointed? Has appointment certificate been returned?	
ii) Have key employees seen the plan and are all employees aware that there is such a plan?	
iii) Have employees been trained to standards for their roles and responsibilities if the business resumption plan is put into effect?	
iv) Does the business resumption plan include contact information for key employees, especially after hours? Local emergency services providers?	
v) Does the plan include provisions for orders of succession?	
vi) Does the business resumption plan include provisions for people with special needs?	
<b>b) Building, Utilities and Transportation</b>	
i) Does the business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?	
ii) Does the business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.	
iii) Review any agreements for use of backup facilities. Are other agencies planning to use the same facility for backup? If yes, can the facility accommodate both agency needs?	
iv) Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?	
v) Does the business resumption plan consider the failure of electrical power, natural gas, telephone service, toxic chemical containers, and pipes?	
vi) Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.	
<b>c) Business Process</b>	
i) Have the business continuity and recovery processes of your agency been addressed in your plan?	
ii) Have the business process or processes been assigned a priority?	
iii) Have employees been assigned by name or by position in the process task order sequence?	
iv) Does the time duration on each task order seem reasonable?	
v) Do the summary of business processes cross-check to the number of process tasks?	
vi) Does the process call tree reflect an order of succession?	
vii) External contact list does it mention contacting the Governor's office?	
viii) Does the resource requirements meet the business process task requirements?	
ix) Can the business process meet the broadest range of customer needs?	
x) The timing of technology requirements sequence appropriately to the delivery of business services?	



<b>c) Information Technology</b>	
i) Determine if the plan reflects the current IT environment.	
ii) Determine if the plan includes prioritization of critical applications and systems.	
iii) Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.	
iv) Does the business resumption plan include arrangements for emergency telecommunications?	
v) Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?	
<b>d) Administrative Procedures</b>	
i) Does the plan contain all the elements identified in the sample plan outline on page 16 of the guidance document (introduction, basic plan and functional annexes)?	
ii) Does the business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time?	
iii) Is there a designated emergency operations center where incident management teams can coordinate response and recovery?	
iv) Determine if the business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.	
v) Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?	
vi) Does the business resumption plan include the names and numbers of suppliers of essential equipment and other material?	
vii) Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the need arise.	
viii) Has the agency conducted an exercise of the plan?	



## Planning and Preparation

### *Identify Critical Agency Products, Services and Operations*

This information will help you assess the impact of an event and determine the need for backup systems. Areas to review include:

- Facilities – Emergency Operating Center and support service areas
- Vendors or third party service providers
- Mandated services, products and required equipment to produce them
- Products and services provided by vendors and contractors
- Lifeline services such as electrical, water, sewer, gas, telecommunications
- Equipment, IT hardware and related infrastructure, contractors
- Essential personnel vital to the function of the facility

### *Identify Internal Resources and capabilities*

Determine how you will address shortfalls and problem areas. Resources that could be used during an emergency response event and/or recovery operation include:

Personnel – fire brigade, security, emergency medical technicians, emergency management officials, public information officers, Community Emergency Response Teams. Determine lines of authority and succession for each position.

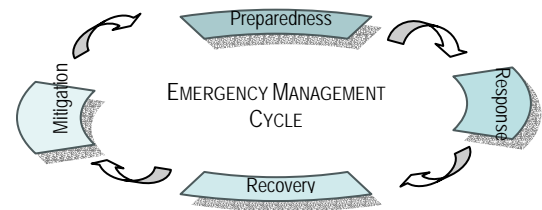
Equipment – fire suppression equipment, first aid supplies, warning system and signals, generators, decontamination equipment etc.

Facilities – Operations Center, media briefing room, sanitation facilities etc.

Organizational capabilities – training, support system, survey staff for foreign language, emergency medical capability etc.

Backup system – arrange to process by critical business services first, then essential services followed by administrative services for:

- |                                   |                                    |
|-----------------------------------|------------------------------------|
| ▪ Agency Personnel                | ▪ Customer services                |
| ▪ Information Systems and support | ▪ Communications                   |
| ▪ Security                        | ▪ Recovery support and assistance  |
| ▪ Emergency power                 | ▪ Agency specific support services |



## THREAT ANALYSIS

Determine the events and environmental impacts that can adversely affect the organization and its facilities. Damage from such events can cause the controls needed to prevent or minimize the effects of a potential loss.

### Threat Identification

Agencies of state government, their facilities and equipment are vulnerable to numerous hazards associated with human caused, naturally occurring and/or technology cyber-crime and cyber terrorism activities. By utilizing an all-hazards, functional approach to planning, the requirement to develop separate plans for every potential threat can be eliminated. Identify the potential hazards and cyber threats in your area based upon your location, conditions and exposure level in the state as well as inquiries to the Statewide Infrastructure Protection Center (SIPC)<sup>3</sup>. Probability and potential impact should also be included such as:

- A small dormant volcano in northern Arizona would have both low probability and low impact.
- Flooding in a metropolitan area could have high impact and high probability to cause excessive property damage.
- Severe winter storms will have a major impact in the northern portion of the state but provide only a limited threat to the southwestern area of Arizona. Organizations like Arizona Department of Transportation or Arizona Department of Economic Security maintain office locations throughout the state and need to plan accordingly.
- Work place violence could have high impact and high probability to occur, regardless of urban or rural areas

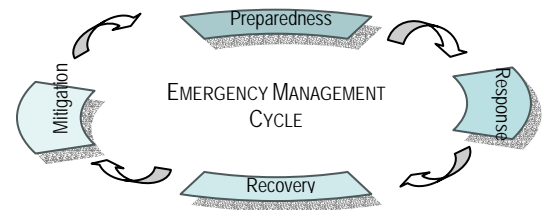
### Property Protection

Determine needs for systems to detect abnormal situations, provide warnings and protect people and property. Consider systems that will provide:

- Fire safety and carbon monoxide protection
- Lighting protection
- Water level monitoring
- Automatic shutoffs
- Emergency power generation
- Special intrusion detection and protection systems

---

<sup>3</sup> SIPC is a function of ADOA/ISD Information Security Services, to become a member please go to <http://www.security.state.az.us/state-Infrastructure.htm>."



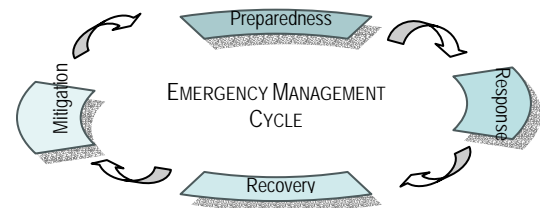
## EMERGENCY COORDINATION

### Coordinate with Emergency Service Providers and Stakeholders

Meet with community emergency services providers and stakeholders to review your existing plan, operational procedures and supporting checklists. Fire service and police officials will have insight into local conditions and how best to mutually support agency emergency operations and life safety initiatives. Establish checklists and or guides (protocol) for turning emergency response activities over to local authorities. **Determine types of business disruptions that exceed the ability of your staff response capability, the activation criteria of your agency plan and the action required to seek additional outside assistance immediately.**

The Emergency Services Coordinator, representatives from community based organizations and local emergency services providers should meet periodically to review mutually supportive issues. Include their roles and joint responsibilities in supporting preservation of public health and safety under emergency conditions. Stakeholders may include representatives from the following organizations:

- Local, county and state emergency services and homeland security officials
- Local Emergency Planning Committees (Hazardous Materials)
- Fire Department and Emergency Medical Services
- Emergency Medical Services
- Public works
- Utilities
- Neighboring agencies, communities of interests
- Risk management
- Police/Sheriff/Capital Mall Security
- Information Technology Coordinator
- Statewide Infrastructure Protection Center – SIPC (ADOA/ISD/Security)
- Maintenance/Building Engineers
- Hospitals and emergency care facilities
- Insurance review
- Special needs support organizations
  - Hearing, vision, mobility impaired and mental/physically disabled
  - Children and seniors, etc.
- Agencies with shared Mutual Aid Agreements
- Third Party Vendors/Support (facilities, etc.)



## Emergency Procedures

These procedures outline how the facility will respond to emergencies and disruptions to business functions. They should appear in the back of your Business Continuity Plan as annexes to your plan. One option is to develop supporting checklists or *Standard Operating Procedures (SOP)*. SOPs determine what *specific* actions would be necessary to, but not limited to:

- Triggers to activate the response teams and mobilize the Operations Center (OC) (See Appendix A)
- Assess an emergency or emerging condition
- Protect staff, the public, property and equipment
- Operating an agency Operations Center
- Warning employees and the public in and around facilities
- Communicating with employees
- Communicating with emergency providers
- Communicate with external audiences
- Conducting evacuation and accounting for staff and public
- Managing initial agency response activities
- Shutting down operations to protect Information Technology
- Communications with Statewide Infrastructure Protection Center (SIPC)
- Protecting vital records and documents
- Order of succession

These items can be grouped into four categories: protection of personnel, containment of the incident, assessment of the effect, and optimum decision actions.

### *Command and Control*

The system for managing emergencies, resources and decision-making is called command and control. Senior managers supporting this process should have the authority to:<sup>4</sup>

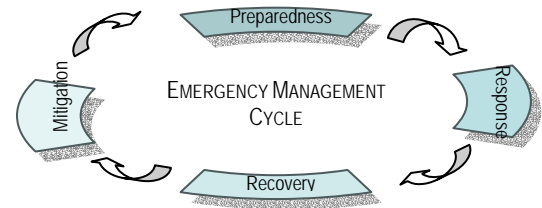
- Implement the plan and activate the agency operations center
- Declare an agency emergency, see Appendix B, Severity Level 1, 2 or 3
- Direct response activities (evacuation)
- Assess the impact of events on the agency
- Shut down a facility
- Activate agency resources and interface with emergency providers
- Issue press releases

---

<sup>4</sup> The State of Arizona supports the development of the National Response Plan, National Integrated Management System (NIMS) and the Incident Command System as a structured framework for emergency response and recovery functions.



## PHASE II



- Declare the event terminated

### ***Critical Emergency Documentation***

#### 1. Emergency Contacts

Create multiple contact lists, including a wallet size card to incorporate 24-hour phone numbers of key staff

#### 2. Building and Site Maps that Include:

A roster of the location of the following information for either a state or leased property facility:

- Utility shutoffs
- Water hydrants, lines and main valves
- Gas main lines and valves
- Electrical cutoffs
- Storm drains
- Sewer lines
- Street name location and address of each building
- Floor plans with escape routes and stairways
- Alarm system
- Fire extinguishers
- Restricted areas
- High-value material or sensitive areas

#### 3. Resource Lists

Prepare resource lists to include major assets (equipment, materials, services, contractors) that could be utilized during an emergency based upon past emergency requirements, real events or projected activities.

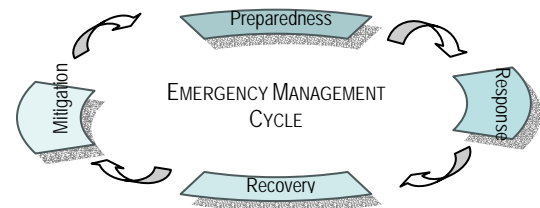
#### 4. Life Safety

Protection of health and safety of everyone in the agency is the first priority during an emergency. One method of protection is evacuation. Building evacuation warnings must be easily understood, routes publicly posted and tested according to schedule.

#### 5. Security

Isolation of the scene should begin when hazards are first discovered or as emerging events threaten the security of a facility. Access should be controlled without placing anyone in physical danger. Trained personnel should perform advanced security control measures to further protect the staff and facility. Initial secure measures should include:

- Closing doors windows and vents
- Create temporary barriers for doors and windows to limit access



- Schedule security guards
- Safely distributing containment material
- Closing file cabinets and desk drawers
- Establish procedures with authorities for facility access
- Understand business requirements to aid in physical asset recovery where appropriate

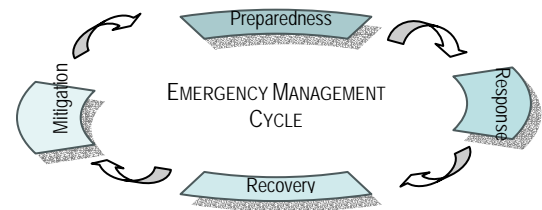
### 6. Operations Center (OC)

The agency OC serves as the central point for emergency operations for your agency. Key senior managers based upon information provided by the staff as well as local emergency providers make decisions here. The OC should be located in an area not likely to be involved in an incident. A conference room or classroom would make a suitable location. Access to the OC should be restricted. Agency decisions, supporting actions and deviations from policy should be timed and noted in a log. The OC should contain the following minimal material necessary to sustain agency emergency operations:

- Agency Business Continuity Plan, SOPs, checklists and guides
- Designated communications equipment
- Reference material
- Activity and call logs
- Plotting boards with dry erase markers
- Conference tables and chairs

“Washington, D.C. alone cannot protect the homeland, just as a town alone cannot rebuild itself after a hurricane or a flood. The key to disaster recovery, and much more importantly, the key to prevention, is mutual cooperation: Sharing resources - equipment, supplies, training and people.”

DHS Sec. Tom Ridge  
Lake Harmony, PA  
September 21, 2004



## INCIDENT MANAGEMENT

### Plan Activation

A wide range of events has the potential to impact on your agency and trigger the activation of your plan. Who has the authority to trigger an activation of your plan and mobilize your Operations Center? Priority action should be focused on threats to agency operations, staff health and public safety. Protection and preservation of real property and assets owned by the state is the second priority after life safety. Activity associated with triggering activation of your plan and operations should be outlined in Annex 2 and 3. Media relations, internal and external communications should be developed as a separate annex.

### Communication

Plan for short to long-term communications failure. Your plan should consider emergency communication between:

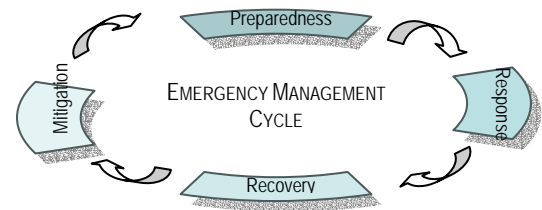
- Emergency providers and the agency OC
- OC and employees
- OC employees' families
- OC and the media
- OC and stakeholders
- OC and the Statewide Infrastructure Protection Center (SIPC)

### Administration and Logistics

Maintain complete and accurate records reflecting initial emergency response by the agency thru the end of recovery operations. Administrative activity prior to and during an emergency may include:

- Documenting drills, exercises and their critiques
- Maintaining detailed records/logs of events in the OC
- Provide facility maps to emergency services providers
- Coordinating support with local Emergency Medical Services
- Providing backup communication, power and transportation
- Supporting Information Technology
- Incident reporting to Statewide Infrastructure Protection Center (SIPC)
- Processing emergency funding and requisitions

The physical and emotional well-being of agency staff should be considered throughout the conduct of agency response and recovery operations. Particular attention should be directed at emerging staff welfare and morale issues at the conclusion of events that involve physical, emotional trauma or extended overtime conditions for agency staff. A staff debriefing should be made available to personnel to assist them in adjusting to



traumatic conditions after a critical incident. Support for arranging these sessions is available from the Arizona Division of Emergency Management.

### **Incident Command**

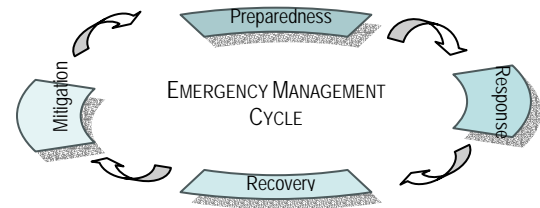
Management of the incident ensures that resources are allocated and decisions are made. Activities include:

- Conduct periodic staff briefings
- Activate personnel notification procedures
  - Develop pre-scripted messages to the staff and public
- Conduct investigation with appropriate agencies
- Staff assignments
- Response and recovery planning strategy
- Insure clarity of command
  - Incident organizational structure
  - Incident objectives
  - Incident Action Plan (IAP)
  - Individual roles
  - Staff support functions

### **After Action Reports**

An After Action Report on steps taken by the agency to manage emergency conditions is imperative to document protective actions taken and provide an historical record for the future. The report should include a chronology of events, lessons learned, potential changes to your BCP and recommendations for improvements to your emergency preparedness program. Reports should be sent to the Arizona Division of Emergency Management as previously listed address and remain a permanent part of agency BCP files.

After completion of your agency emergency recovery efforts, following either an activation of your BCP plan or a major exercise, a staff incident de-briefing should be conducted to institutionalize lessons learned from real or simulated events. A record of this review should be developed and remain in your BCP file in the form of an After Action Report. Refer to Appendix E for sample format.



## BUSINESS CONTINUITY AND RECOVERY

After a business disruption event occurs and employee safety is assured, business restoration becomes the primary focus. The scope of the disruption, single location or community-wide, will determine the individuals activated and the duration of the activation. To expedite the response in this stage, the Emergency Services Coordinator should prepare a streamlined system to report damage and establish priorities.

### Damage Assessment

The agency BCP should provide adequate instructions that coordinate this effort with the agency loss control representative and ADOA's Risk Management staff to ensure the proper collection of information such as:

- Inventory property and determine losses
- Document damaged equipment, records, photographs, etc. with a camera
- Maintain detailed records for repair/replacement of material
- Identify appropriate methods to protect undamaged equipment and material onsite
- Prepare procedures for stabilizing and reclaiming water/smoke damaged assets and records
- Remove debris and damaged equipment from facilities
- Conduct salvage operation and assess value

### Salvage and Restoration

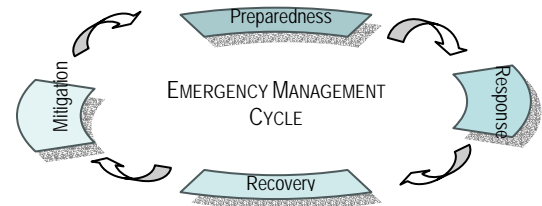
Photograph or videotape facilities to document agency assets prior to the occurrence of an event. Update these files regularly to accurately reflect assets and their condition. The salvage and restoration processes may include:

- Repairing or replacing equipment
- Relocating to an alternate site
- Contracting operations or engineering services
- Records and document preservation
- Risk management and insurance issues

### Business Processes

The goal of Business Continuity Planning is recovery and restoration of agency services following a disruptive event. After emergency actions are complete, initiate plans to resume to normal operations. Appoint a recovery team of managers to complete a preliminary damage assessment, establish priorities, initiate additional

## PHASE II



protective actions and coordinate restoration efforts. In Phase 1 of your plan you were asked to identify the following information:

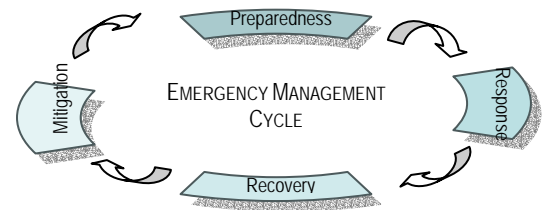
- 4 – Business Process Information*
- 5 – Business Information and Documents*
- 6 – Process Tasks*
- 7 – Process Call Tree*
- 8 – Internal Agency Dependencies*
- 9 – External Dependencies*
- 10 – External Contacts*
- 11 – Customer Contact*
- 12 – Recovery Team Personnel*
- 13 – Business Equipment and Supplies*
- 14 – Information Technology Applications*
- 15 – Information Technology Server/Hardware*
- 16 – Telecommunications*
- 17 – Alternate Sites*

### **Return to Normal Operations**

After resuming business, it may take month or years to restore operations to normal. Many factors will be out of your control, such as insufficient community redevelopment plans, delays in issuing building permits, and shortages in supplies and equipment. Anticipate roadblocks such as these in your plans.

### **Communication**

Plan for short to long-term communications failure. Consider your daily operations and the impact of voice and data transmissions on operations. What is the business impact of a systems failure? Determine backup communication for each business function. Establish procedures for restoring services with vendors. Alternate means of communications include messenger, two-way radio, FAX machine, local area networks, cell phone, satellite phones, etc. Capitol mall agencies have a priority for restoration of telephone service. Please note cell phone usage may be severely limited.



## TRAINING PLAN

### Employee Orientation and Training

Determine and assign staff responsibility for developing a training plan with specific assignments and milestones:

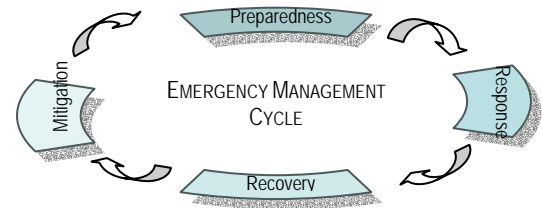
- Who will be trained at what level?
- Who will do the training?
- When and where training will take place?
- How will training be evaluated and documented?

Provide an orientation to all agency staff and outline the procedures and features established in your revised Business Continuity Plan. Training should consist of task identification, standards to be accomplished and conditions under which they will operate. Do personnel know what they should do in an emergency? Training should be sanctioned by supervisors, budgeted and designed to reinforce the agency plan. Accounting for human costs (such as, overtime for Fair Labor Standard Act employees, or extra materials purchased in the event of future disasters) and tracking of training results should be monitored. Staff assignments should be noted on agency Position Description Questionnaires. A staff orientation session should include time for group discussion and questions from the staff. Not all safety and preparedness information should be shared or made available in open discussion.

Training should address the following issues (not prioritized):

- Individual roles and responsibilities during an emergency
- Prepare handouts on job descriptions for future reference
- Information about local hazards and threats
- Alert, notification, and warning procedures
- Protocol for locating family members
- Emergency response procedures
- Location, use, and maintenance of emergency equipment
- Fire extinguishers, airways, first aid supplies etc.
- Shut down, evacuation, and emergency protective action procedures
- Security Awareness, suspicious activity deviating from norm
- Family preparedness – American Red Cross
- Hazard vulnerability
- Risk management and loss prevention

## PHASE II

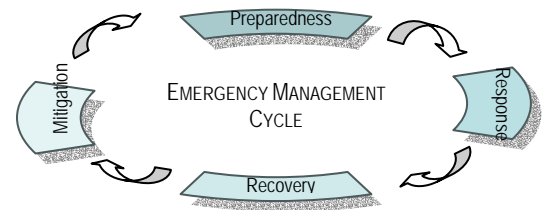


Hazard specific conditions or topics should include:

- Fire or explosion
- Hazardous materials incidents
- Severe storms
- Floods
- Earthquakes
- Technological emergencies
- Terrorism
- Acts of war
- Accidents
- Utility outages
- Heating/cooling failure
- Computer system failure
- Contamination
- Prohibited access to facility
- First Aid
- Loss of Key agency personnel.

The American Red Cross is available to provide basic awareness level emergency preparedness training to aid in your employee orientation training. Additional information concerning their potential involvement in your awareness level training will be available at our Orientation Seminar. Contact the Grand Canyon Chapter of the American Red Cross to invite them to conduct their training at (602) 336-6660 <http://www.arizonaredcross.org>





## EXERCISE AND REVISE

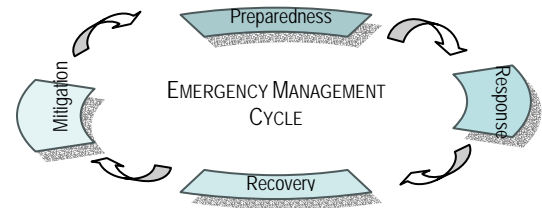
After your staff has completed an orientation session on the agency's revised Business Continuity Plan and individuals with specific response authority have received instruction and training on their functions, an agency tabletop exercise should be conducted. See Appendix D for a model training outline.

### Tabletop Exercise

Tabletop exercises are used to simulate the effectiveness of your plan, operating procedures and supporting operational protocol. A tabletop exercise with senior staff and your ESC will serve as a diagnostic tool to evaluate the strengths and weaknesses of your emergency management program. In the room designated as your Operations Center, a facilitator should describe a series of emergency events (scenario) and have participants describe how they would react according to your plan and procedures. The scenarios used in designing your tabletop exercises and creating discussion points should be developed based upon your vulnerability analysis, case studies and actual events. A discussion should follow to evaluate your actions, plan, emergency operating procedures and staff training provided under these emergency conditions. Identify areas of confusion, overlap or realignment that would strengthen your plan. Were you able to successfully manage problems when emergency conditions continued to cascade?

#### EXERCISE PLANNING OUTLINE

1. Develop realistic scenarios
  - a. Create exercise scenarios to resemble types of incidents the organization is likely to experience
  - b. Define assumptions and limitations
2. Establish exercise evaluation criteria
  - a. Develop criteria aligned with exercise objectives and scope that are measurable and both qualitative and quantitative
  - b. Identify expected results for comparison analysis
3. Conduct Exercise
4. Post-Exercise Reporting
  - a. Create a comprehensive After Action Report (AAR) with recommendations and forward a copy to ADEM
  - b. Update plan per recommendations

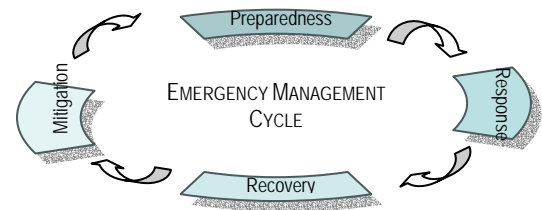


### Functional Exercise

These exercises evaluate specific emergency functions outlined in the annexes to your plan such as notifications and communications. Personnel are asked to respond to scenario inputs at your OC and determine a course of action based on real time events. A critique is held at the conclusion of the session to identify problem areas and system status.

Revise/modify your plan to reflect changes identified in your review process and tabletop exercise. Consider the following issues:

- Does the plan reflect lessons learned from recent events and exercises?
- Does staff have a clear understanding of their role and responsibilities?
- Does the plan reflect changes to facilities and processes?
- Are photographs of critical equipment current?
- Have training objectives been accomplished?
- Does notification information remain current and accurate?



## MAINTENANCE AND CONTINUOUS IMPROVEMENT PLAN

### Operational Integration

Your plan should remain a vital and dynamic part of your agency's emergency preparedness program and should be integrated into your routine day-to-day operations. Steps should be taken to build emergency preparedness awareness and continue the planning, training and exercise cycle annually in your agency as an integral part of your management culture every year.

Communicate with other agency administration and share mutual concerns and observations concerning your Business Continuity Plan and preparedness program. A management program audit should be conducted on an annual basis to include:

- Update notifications changes
- Identify communities of interest and mutual aid support
- Incorporate new information and lessons learned into your procedures
- Maintain a vulnerability analysis
- Verify order of agency management succession (chain of command) plan.

### Annual Plan Updates and Audit

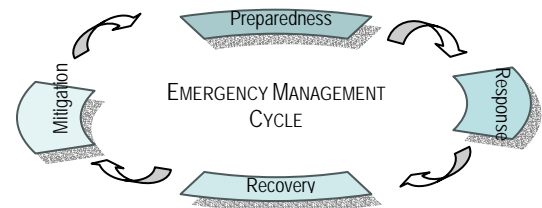
During your annual formal audit of your Business Continuity Plan consider the following initiatives:

- How to involve all levels of management in evaluating the plan?
- Are the shortfalls previously identified addressed in your current plan?
- Does the plan reflect lessons learned from exercised and real events?
- Does the plan reflect current processes and procedures?
- Are photographs and facility maps up to date?
- Have the threats or hazards in the facility changed?
- Have current year training objectives been met?
- Are the contact phone numbers accurate?

Provide a plan briefing by the emergency planning team for the agency director and senior management. Secure written approval of the updated plan and annual training and exercise activities proposed in support of the agency's emergency management program.

Print/duplicate and assemble the plan in three ring binders, number all pages and copies of the plan. The plan should be identified for *Official Use Only*, secured and maintained as a sensitive document. Secure file copies on a CD Rom format. The updated plan

## PHASE II



should be provided to: agency director and senior managers; agency assigned emergency response personnel and community emergency services providers. Every individual receiving a copy should sign a receipt and post additional changes and updates to their plan. Key personnel should keep an additional copy at their residence.

### Compliance

Identify and maintain applicable files for federal, state and local regulations such as:

- Environmental regulations
- Fire and life safety codes
- Occupational safety and health regulations
- Zoning regulations
- Agency policies
- Federal, State and local statutes and administrative rules.

#### **THE FREEDOM OF INFORMATION ACT (FOIA)**

FOIA is a federal statute and generally provides that any person has a right to request access to agency records, except to the extent the records are protected from disclosure by any of nine exemptions contained in the law or by one of three special law enforcement record exclusions.

#### **FOR OFFICIAL USE ONLY (FOUO)**

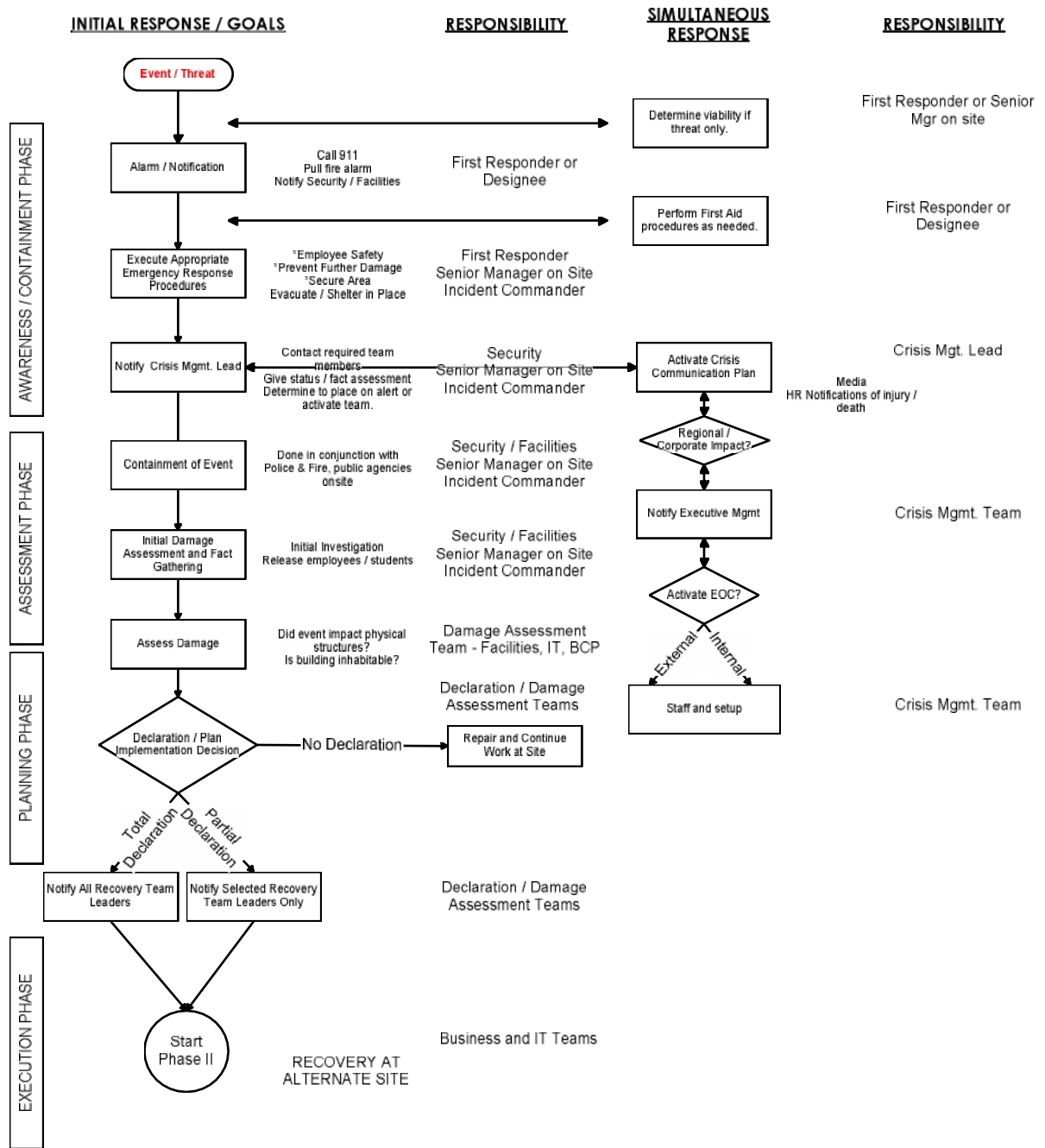
FOUO is the designation used on official information not requiring a security classification but which must be withheld and protected from public release. Unclassified messages containing FOUO information must have the abbreviation “FOUO” after the designation “UNCLASS.”

See Appendix E

# APPENDIX A:

## TRIGGER/RESPONSE FLOW CHART

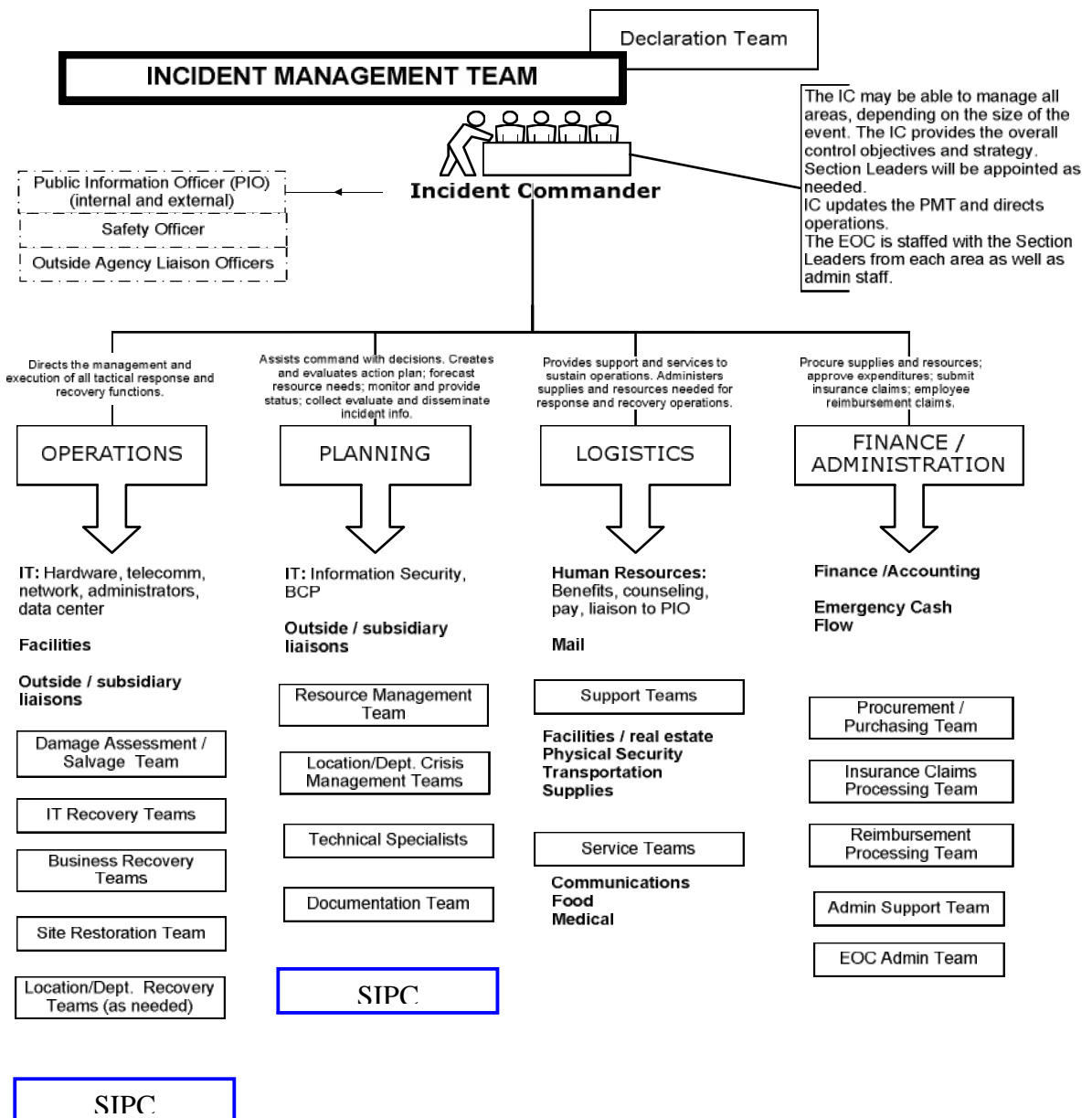
### Incident Response / Notification



## APPENDIX B:

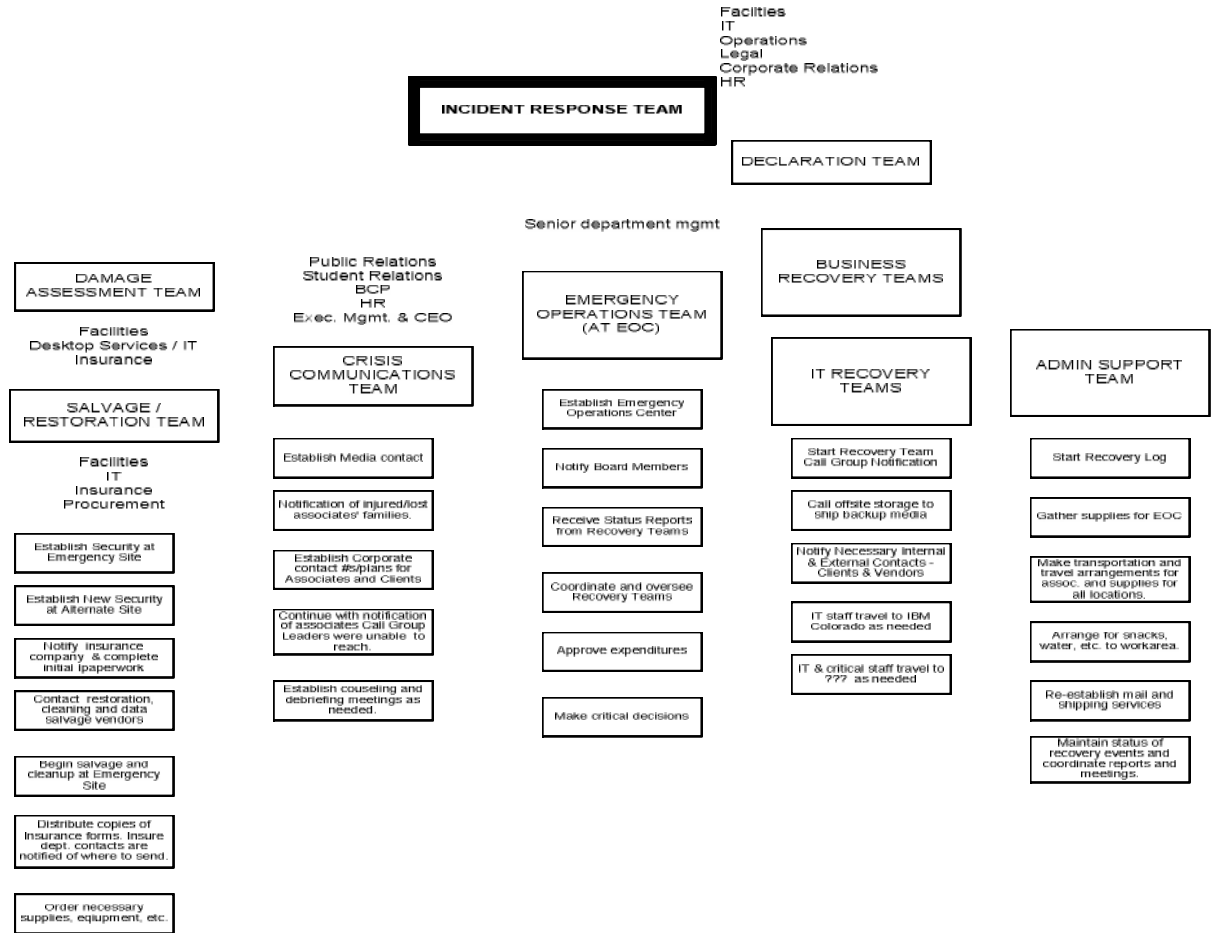
### POLICY MANAGEMENT TEAM

The PMT will establish policy & priority guidelines to the IMT, enabling them to implement approved response and recovery strategies to mitigate further damage to employees, the facility, data, and public perception. Each member will provide direction for their respective business departments.



## APPENDIX C:

### PROPOSED TEAM STRUCTURE



---

## APPENDIX D:

### ***DISASTER RECOVERY PLANNING (DRP) FOR IT***

Information Technology (IT) and automated information systems are vital elements for the majority of business programs and processes that serve the public, state, and other third party organizations. Because IT resources are essential to the success of the state, it is critical that services provided by these technologies are able to operate effectively without excessive interruption.

Disaster Recovery Planning (DRP) for IT represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. DRP fits into the broader Business Continuity Planning (BCP) and together completes a holistic plan for the resumption of state business programs and services. Ultimately, an IT Unit within a state agency will use a suite of plans to properly prepare for recovery and continuity activities for disruptions affecting IT systems, business processes, and various facilities. Because of the inherent relationship between IT systems and the business programs/processes, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts with the overall Business Continuity Plans (BCP).

Agencies (or budget units) that have implemented an automated Disaster Recovery Planning system (Commercial Off the Shelf (COTS) or Government Off the Shelf (GOTS)) comply with the requirements and section of this guideline. All other Budget Units without an automated system must comply with this guideline.

### **Preventive Controls for Information Technologies**

Cyber-crime, terrorism and disaster activities may have a better chance of being mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. A wide variety of preventive controls are available, depending on system type and configuration; some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components such as servers (mainframe, midrange and network servers) storage devices (DAS, NAS, SAN), and end-user-devices (workstations/PC laptops, etc.).
- Surge protectors to protect end-user-devices.
- Gasoline or diesel powered generators to provide long term backup power.
- Air condition systems with adequate excess capacity to permit failure of certain components, such as a compressor.
- Store software copies of critical software applications and data/information with related documentation off-site with corresponding licensing agreements.



### Appendix D continued

- 
- Install anti-virus software on workstations/Laptops and update software patches on a periodic basis
  - Install anti-spy ware software on each workstations/laptops and update software patches on a periodic basis
  - Update operating systems software patches on servers (mainframe, midrange and networks servers) and end-user-devices (workstations/PC laptops, etc.) on a periodic basis
  - Control physical access to servers (mainframe, midrange and network servers) storage devices (DAS, NAS, SAN), and end-user-devices (workstations/PC laptops, etc.)
  - Install fire suppression systems
  - Install fire and smoke detectors
  - Install water sensors in the computer room ceiling and floor
  - Plastic tarps that may be unrolled over IT equipment to protect it from water damage
  - Heat resistant and waterproof containers for backup media and vital non-electronic records
  - Emergency master system shutdown switch
  - Offsite storage of backup media, non-electronic records, and system documentation
  - Technical security controls, such as cryptographic key management and least privilege access controls
  - Frequent, scheduled backups to include periodically tested recoverability
  - Become a member of the Statewide Infrastructure Protection Center of ADOA, and receive alert notifications on cyber-crime and terrorism activities as well as reporting significant incidents to SIPC.

### **Develop Recovery Strategies**

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. Strategies should address disruption impacts and maximum outage times (MAO) identified in the Business Continuity planning templates. Several alternatives should be considered when developing the strategy, including costs, allowable outage times, security, and integration within the Business Continuity Planning (BCP) guide. IT units that comply with the suite of statewide IT security policy and standards will be in a state of preparedness and readiness for BCP and DRP planning.

#### ***Backup Methods***

Backup methods with respect to frequency, media, off-site storage, content, and procedures shall comply with the statewide IT security standard P800-P870 Backups.

### Appendix D continued

---

#### *Alternate Sites*

Although major disruptions with long-term effects may be rare, they should be accounted for in the DRP plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period and is the responsibility of the state agency to negotiate and implement. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the Budget Unit
- Reciprocal agreements with other Budget Units or third party
- Commercially leased facility

Regardless of the type of alternate site selected, the facility must be able to support system operations and the resumption of business programs and processes even if limited to some extent.

#### **Hardware/Software Replacements**

IT systems that are damaged/destroyed and if primary/secondary sites are unavailable, necessary hardware and software and possibly consulting help will need to be activated or procured quickly and delivered to the primary and/or alternate location. Please refer to the State Procurement Office web-site at [www.azspo.az.gov](http://www.azspo.az.gov). when selecting the most appropriate procurement strategy.

- ***Statewide IT Contracts*** – A variety of statewide IT contracts for IT equipment and services available to the state.
- ***Volume, Enterprise and Other Software License Agreements*** – A variety of statewide IT software license agreements are available to the state.
- ***Microcomputer Hardware, Software and Services Contracts*** – Value Added Resellers (VARs), and Direct Manufacturer's (DMs) offer a variety of products and free services available to the state.
- ***IT Consultant Services Contract*** – Available in thirty-eight different categories that includes Database managers, Web Developers, LAN/WAN Administrators, Technical Support Specialists, Programmer Analysts, etc.

#### **IT Incident/Recovery Teams**

Having selected the system recovery strategy the CIO must designate the appropriate teams to implement the strategy. Recovery personnel should be assigned to one of several specific teams that will respond to the event, recovery capabilities, and return the system to normal operations. The specific types of teams required are based on the systems affected. Recovery teams will require some or all of the following functional group

- Senior Management
- Management Team
- Damage Assessment Team
- Operating Sys Admin Team
- System Software Team
- Server Recovery Team
- Database Recovery Team

## PHASE II

### Appendix D continued

---

- Network Ops Recovery Team
- Applications Recovery Team
- Telecommunications Team
- Alternate Site Recovery Coordinating Team
- Test Team
- Media Relations Team
- Legal Affairs Team
- Physical/Personnel Security Team
- Procurement Team
- Hardware Salvage Team

Each team is led by a team leader who directs overall team operations and acts as the team's representative to management and liaisons with other team leaders. The team leader disseminates information to team members and approves any decisions that must be made within the team.

---

## APPENDIX E

### *AFTER ACTION REPORT*

**State of Arizona**  
**AFTER ACTION REPORT**  
**for**

---

#### **CONTENTS**

**I. AFTER ACTION NARRATIVE:**

- A. Mission Statement**
- B. Goals and Objectives**
- C. Workshop Timeline**
- D. Target Audience**
- E. Implementation & Logistics**

**II. SUMMARY OF EXERCISE**

**III. Feedback, Comments & Suggestions**

**IV. Lessons Learned**

**V. Attachments**

---

## APPENDIX F

### ***TASK TRAINING OUTLINE***

#### **Steps - Model procedure for each task to be trained:**

1. Define Training Objective according to the task, condition and standard
  - a. Reference documents
  - b. Supervisor's direction and guidance
2. Assemble Training Resources and Materials
  - a. Secure training facility and equipment
  - b. Identify trainers
3. Prepare Training and/or Demonstration
  - a. Develop performance steps and training outline
  - b. Model training program
4. Conduct training
  - a. Provide orientation demonstration, skill practice and feedback, pretest
  - b. Performance test
5. Document training
  - a. Record and report training results
  - b. Input to supervisors and EMC on results

## APPENDIX G:

***Disclaimer:***

*The following federal directive establishes policy concerning identification, safeguarding and distribution of sensitive but unclassified information. It is included here for your information and reference only. Its inclusion is not intended to replace existing agency policy. Each agency should adopt a state approved policy concerning storage, security, distribution and maintenance of sensitive material in their BCP.*

### **SAFEGUARDING (FOR OFFICIAL USE ONLY) INFORMATION**

#### **1. Purpose**

This appendix establishes a model for controls regarding the identification and safeguarding of sensitive but unclassified information. It also applies to other sensitive but unclassified information received from other government and non-governmental activities.

#### **2. Definitions**

**Access:** The ability or opportunity to gain knowledge of information.

**For Official Use Only (FOUO):** The term used within an agency to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest.

**Need-to-know:** The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

#### **3. Responsibilities**

Be aware that divulging information without proper authority could result in administrative or disciplinary action. Supervisors and managers will:

Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.

#### **4. Policy and Procedures**

##### A. General

Appendix G continued

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency.
2. Designation of information as FOUO is not a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.
3. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

B. For Official Use Only

Within an agency, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information within the community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation, as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.
  - (a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.
  - (b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.

Appendix G continued

- 
- (c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.
  - (d) Other international and domestic information protected by statute, treaty, regulation or other agreements.
  - (e) Information that could be sold for profit.
  - (f) **Information that could result in physical risk to personnel.**
  - (g) **Information technology (IT)** internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.
  - (h) **Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.**
  - (i) **Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.**
  - (j) Developing or current technology, the release of which could hinder the objectives of government, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

D. Designation Authority

Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

F. Marking

Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of



Appendix G continued

---

the material will protect it as FOUO. Other sensitive information protected by statute or regulation, will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

1. Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."
2. Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

*WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.*

3. Materials being transmitted to recipients outside federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

*WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized official.*

4. Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."
5. Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).
6. Individual portion markings on a document that contains no other designation are not required.
7. Designator or originator information and markings, downgrading instructions, and date/event markings are not required.

### G. General Handling Procedures

Although FOUO is the government standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Additional control requirements may be added as necessary to afford appropriate protection to the information. Employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 6.1) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL IJSE ONLY" cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.
2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.
3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

### H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically to unauthorized personnel.
2. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator.
3. The holder of the information will comply with any access and dissemination restrictions.
4. A security clearance is not required for access to FOUO information.
5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions

## PHASE II

### Appendix G continued

---

- are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.
6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable agency program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know.
  7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.
  8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.
  9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

#### I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.
2. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems Publication 4300A.

#### J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:
  - (a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of

Appendix G continued

---

- tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).
- (b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.
  - (c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.
2. Electronic Transmission.
- (a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.
  - (b) Transmittal via E-Mail
    - (i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.
    - (ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.
  - (c) DHS Internet/Intranet
    - (i) FOUO information will not be posted on an internet (public) website.
    - (ii) FOUO information may be posted on the intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked

Appendix G continued

---

as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:
  - (a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.
  - (b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.
  - (c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. Additional notifications to appropriate management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.
2. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

## ACRONYMS

AAC	Arizona Administrative Code	AZSERC	Arizona State Emergency Response Commission
ACC	Arizona Corporation Commission	AzVOAD	Arizona Voluntary Organizations Active in Disasters
ACEP	American College of Emergency Physicians		
ACOS	American College of Surgeons	BCP	Business Continuity Plan
ADA	Arizona Department of Agriculture	BHD	Behavioral Health Division
ADA	Arizona Dental Association		
ADC	Arizona Department of Commerce	CAP	Civil Air Patrol
ADE	Arizona Department of Education	CAS	Chemical Abstract System
ADEM	Arizona Division of Emergency Management	CBR	Chemical, Biological, Radiological
ADEQ	Arizona Department of Environmental Quality	CDC	Centers for Disease Control
ADES	Arizona Department of Economic Security	CERCLA	Comprehensive Environmental Response Compensation & Liability Act
ADHS	Arizona Department of Health Services	CES	Cooperative Extension Services
		CFR	Code of Federal Regulations
ADOA	Arizona Department of Administration	CHEMTREC	Chemical Transportation Emergency Center
ADOC	Arizona Department of Corrections	CHRIS	Chemical Hazards Response Information System
ADOE	Arizona Department of Energy	CISD	Critical Incident Stress Debriefing
ADOT	Arizona Department of Transportation	CISM	Critical Incident Stress Management
ADWR	Arizona Department of Water Resources	CoBRA	Chemical Biological Response Aide
		CRG	Chemical Referral Guide
AOC	Alternate Operations Center	CST	Civil Support Team AZ National Guard
AFCA	Arizona Fire Chiefs' Association		
AFDA	Arizona Funeral Directors Association		
AGCA	Associated General Contractors of America	DEMA	Department of Emergency and Military Affairs
AoA	Administration on Aging	DFO	Disaster Field Office
AP	Assembly Point	DHHS	Department of Health and Human Services
APS	Arizona Park Service	DPS	Department of Public Safety
APS	Arizona Public Service	DST	Damage Survey Team
ARC	American Red Cross	DWI	Disaster Welfare Information
ARRA	Arizona Radiation Regulatory Agency		
ARS	Arizona Revised Statutes	EAS	Emergency Alert System
AZGFD	Arizona Game & Fish Department	EDNA	Emergency Department Nurses Association
AZNG	Arizona National Guard		

## PHASE II

### Acronyms continued

EHTR	Emergency Highway Traffic Regulation	MVD	Motor Vehicle Division
EMS	Emergency Medical Services	NFPA	National Fire Protection Association
EOP	Emergency Operations Plan	NIMS	National Incident Management System
EPA	Environmental Protection Agency	NOI	Notice of Interest
EPCRA	Emergency Planning and Community Right-to-Know Act	NRC	National Response Center
EPI	Emergency Public Information	NRC	Nuclear Regulatory Commission
EPIS	Emergency Public Information System	NRT	National Response Team
ERT	Emergency Response Team	NWS	National Weather Service
		NWWS	National Weather Wire Service
FBI	Federal Bureau of Investigation	OC	Operations Center
FEMA	Federal Emergency Management Agency	OCC	Operations Communications Center
FOSC	Federal On-Scene Coordinator	OSC	On-Scene Coordinator
FRP	Federal Response Plan	OSHA	Occupational Safety and Health Act
		OSPB	Office of Strategic Planning and Budgeting
GAR	Governor's Authorized Representative	PA	Project Application
GEF	Governor's Emergency Fund	PA	Public Assistance
HEW	Health, Education and Welfare, Department of	PAG	Protective Action Guidelines
HPB	Highway Patrol Bureau	PDA	Preliminary Damage Assessment
HUD	Housing and Urban Development	PDD	Presidential Decision Directive
		PIO	Public Information Officer
IC	Incident Commander	PL	Public Law
ICS	Incident Command System	POA	Point of Arrival
INS	Immigration and Naturalization Service	PPE	Personal Protective Equipment
IOP	Internal Operating Procedure	PSP	Pipeline Safety Personnel
		RACES	Radio Amateur Civil Emergency Services
JENC	Joint Emergency News Center	RCRA	Resource Conservation and Recovery Act
JIC	Joint Information Center		
JLBC	Joint Legislative Budget Committee	RM	Resource Manager
JOC	Joint Operations Center	RMS	Risk Management Section
		RP	Responsible Party
LEPC	Local Emergency Planning Committee	SA	Staging Area
LSA	Lead State Agency	SAR	Search and Rescue
LSPIO	Lead State Public Information Officer	SARA	Superfund Amendments and Reauthorization Act
MARS	Military Amateur Radio System	SBA	Small Business Administration
MC	Mobilization Center		
MSDS	Material Safety Data Sheet		

## PHASE II

### Acronyms continued

---

SC	State Clearinghouse	SFM	State Fire Marshall
SCO	State Coordinating Officer	SFSC	State Fire Safety Committee
SEC	State Emergency Council	SILC	Statewide Independent Living Council
SECC	State of Arizona Emergency Communications Center	SIPC	Statewide Infrastructure Protection Center
SOC	State Operations Center	SLD	State Land Department
SERO	State Emergency Response Organization	SOG	Standard Operating Guide
SERRP	State Emergency Response and Recovery Plan	SOP	Standard Operating Procedures
		SOSC	State On-Scene Coordinator
		SWP	State Warning Point



## GLOSSARY

**AFTER ACTION REPORT** – Following each exercise a report documenting the response effort and lessons learned. Each State agency involved in the response will keep records of its activity to assist in preparing their BCP and maintain a file.

**ABC FIRE EXTINGUISHER** - Chemically-based devices used to eliminate ordinary combustible, flammable liquid, and electrical fires.

**ACTIVATION** - When all or a portion of the agency BCP has been put into motion.

**ALERT** - Notification that a disaster situation has occurred—stand by for possible activation of agency BCP.

**ALTERNATE SITE** - A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

**APPLICATION RECOVERY** - The component of disaster recovery dealing specifically with the restoration of business system software and data after the processing platform has been restored or replaced. Similar Terms: business system recovery.

**ASSUMPTIONS** - Basic understandings about unknown disaster situations that the disaster recovery plan is based on.

**ARIZONA VOLUNTARY ORGANIZATIONS ACTIVE IN DISASTERS (AZVOAD)** - AzVOAD is a coalition of voluntary organizations organized at state and local levels. In non-disaster periods, it meets to discuss emergency management issues and encourage cooperation, communication, coordination, and collaboration among voluntary organizations. In the response period, each individual organization functions independently, yet cooperatively.

**BACKLOG TRAP** - The effect on the business of a backlog of work that accumulates when a system or process is unavailable for a long period—a backlog that may take a considerable length of time to reduce.

**BACKUP POSITION LISTING** - A list of alternative personnel who can fill a recovery team position when the primary person is not available.

**BACKUP POWER** - Generally diesel generators used to provide sufficient power to operate equipment normally when commercial power fails.

**BACKUP STRATEGY** - Alternative operating method (i.e., platform, location, etc.) for facilities and systems operations in the event of a disaster.

**BIOLOGICAL AGENTS** - The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.

## PHASE II

### Glossary continued

---

**BUSINESS AS USUAL** - Operating under normal conditions, i.e., without any significant interruptions of operations as a result of a disaster.

**BUSINESS CONTINUITY PLAN** - A predefined collection of procedures and documentation designed to assist an organization to respond to any of a set of disasters, disruptions, or emergencies. The plan provides a mechanism for management and employees to use routine time to carefully consider what actions should be taken under emergency conditions. A contingency plan should contain and describe sufficient management thought and planning such that an employee can implement specific direction in an emergency.

**BUSINESS CONTINUITY PLANNING (BCP)** - An all encompassing, “umbrella” term covering both disaster response and recovery planning and business resumption planning.

**BUSINESS FUNCTION:** The most elementary activities, e.g., calculating gross pay, updating job descriptions, matching invoices to receiving reports.

**BUSINESS IMPACT ANALYSIS (BIA)** - The process of analyzing all business functions and the effect that a specific disaster may have upon them.

**BUSINESS INTERRUPTION** - Any event, whether anticipated or unanticipated which disrupts the normal course of business operations at a agency location.

**BUSINESS RECOVERY PLAN** - A document containing corporate-wide policies and test-validated procedures and action instructions developed specifically for use in restoring company operations in the event of a declared disaster.

**BUSINESS RECOVERY PROCESS** - The common critical path that all companies follow during a recovery effort. There are major nodes along the path that are followed regardless of the organization. The process has seven stages: 1. Immediate response, 2. Environmental restoration, 3. Functional restoration, 4. Data synchronization, 5. Restore business functions, 6. Interim site, 7. Return home.

**BUSINESS RECOVERY TEAM** - A group of individuals responsible for maintaining and coordinating the recovery process

**BUSINESS RECOVERY PLANNING (BRP)** - A “near synonym” for contingency planning. It implies that the plan includes the tasks required to take the organization from the immediate aftermath of a disaster through the return to, or resumption of normal operations.

**CHECKLIST TEST** - A method used to test a completed disaster recovery plan. This test is used to determine if the information, such as phone numbers, manuals, equipment, etc., in the plan is accurate and current.

**CHEMICAL AGENTS** - The FBI WMD Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and animals.

**CHEMICAL TRANSPORTATION EMERGENCY CENTER (CHEMTREC)** - A facility of the Chemical Manufacturers Association located in Washington, D.C. which provides information on dealing with chemical transportation accidents 24 hours per day.

## PHASE II

### Glossary continued

---

**COLD SITE** - An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold sites have many variations depending on their communication facilities, UPS systems, and mobility. Plans employing a cold site provide a time period when teams procure and install equipment prior to the need to use the facility. See also Portable Shell, Uninterruptible Power Supply. Similar Terms: shell-site, backup site, recovery site, alternate site.

**COMMUNITY RIGHT-TO-KNOW** - Legislation requiring the communicating of chemical information to local agencies or the public.

**COMPREHENSIVE ENVIRONMENTAL RESPONSE COMPENSATION AND LIABILITY ACT OF 1980 (CERCLA)** - More popularly known as "Superfund," CERCLA was passed to provide the needed general authority for Federal and State governments to respond directly to hazardous substances incidents.

**COMPUTER RECOVERY TEAM** - A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.

**CREDIBLE THREAT** - The FBI conducts an interagency threat assessment that indicates the threat is credible and confirms the involvement of a WMD in the developing terrorist incident.

**CRISIS** - A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.

**CRISIS EVENT** - An event, which produces a temporary state of psychological disequilibria and a subsequent state of emotional turmoil.

**CRISIS MANAGEMENT** - The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

**CRITICAL BUSINESS FUNCTIONS** - Vital business functions without which an organization cannot long operate. If a critical business function is non-operational, the organization could suffer serious legal, financial, goodwill or other serious losses or penalties.

**CRITICAL INCIDENT** - A critical incident is any event that has a stressful impact sufficient enough to overwhelm the usually effective coping skills of either an individual or a group. Critical incidents are typically sudden, powerful events that are outside of the range of ordinary human experiences. Because they are so sudden and unusual, they can have a strong emotional effect even on well-trained, experienced people.

**CRITICAL INCIDENT STRESS** - The reaction a person or group has to a critical incident. Critical Incident Stress is characterized by a wide range of cognitive, physical, emotional and behavioral signs and symptoms. Most people recover from critical incident stress within a few weeks.

**CRITICAL INCIDENT STRESS DEBRIEFING (CISD)** - A group meeting or discussion about a distressing critical incident. Designed to mitigate the impact of a critical incident and to assist and educate the personnel in recovering as quickly as possible from the stress associated with the

## PHASE II

### Glossary continued

---

event. The CISD is run by a specially trained team which includes peer support personnel and a mental health professional.

**CRITICAL INCIDENT STRESS MANAGEMENT (CISM)** - A wide range of programs and intervention strategies which have been designed to prevent stress in emergency personnel and to assist them in managing and recovering from significant stress should they encounter it in their work. It includes pre incident education, significant-other support programs, defusings, demobilizations, debriefings, on-scene support services, individual consultations, peer counseling, initial discussions, crisis intervention training, disaster preparedness, and other disaster assistance programs.

**CRITICAL INCIDENT STRESS TEAM** - A team of professional and peer personnel who have received special training to intervene in stress reactions.

**CRITICAL RECORDS** - Records or documents, which, if damaged or destroyed, would cause considerable, inconvenience and/or require replacement or recreation at considerable expense.

**DAMAGE ASSESSMENT** - The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced.

**DATA BACKUP** - The process of copying the essential elements of a data processing function, programs, data, data bases, procedures, documentation, etc. Data backup to support any recovery effort must include a storage strategy that physically separates the backup data from the original data, such that there is an absolutely minimal chance that the same event could destroy both copies. Off-site storage in a secure environment is the generally accepted solution.

**DATA CENTER RECOVERY** - The component of disaster recovery that deals with the restoration, at an alternate location, of data center services and computer processing capabilities.

**DATA CENTER RELOCATION** - The relocation of an organization's entire data processing operation.

**DEBRIEFING** - Generic term for the Critical Incident Stress Debriefing (CISD) process.

**DECLARATION** - A formal statement that a state of disaster exists.

**DEDICATED LINE** - A pre-established point-to-point communication link between computer terminals and a computer processor, or between distributed processors which does not require dial-up access.

**DEFUSING** - The defusing is a shortened version of the Critical Incident Stress debriefing. Defusing always take place immediately or relatively soon after the critical incident is finished, and lasts between twenty and forty-five minutes. It is designed to eliminate the need to provide a formal debriefing.

**DEMOBILIZATION - DE-ESCALATION - DECOMPRESSION** - All three words are used as synonyms to mean a brief intervention that is reserved for use immediately after a disaster or other large scale incident. The intervention is designed to provide a transition period from the world of the traumatic event back to the world of the routine. As personnel are relieved from

### Glossary continued

---

their shift, they are sent as a unit to a demobilization center. Here they are given a ten minute talk on critical incident stress, the symptoms they might encounter and some suggestions which will be immediately helpful to them during the next twenty-four to seventy-two hours or until a debriefing can be arranged to discuss the incident. After the ten-minute talk, the emergency workers are sent to another room in which food and non-alcoholic beverages are served. After a twenty-minute rest, the units are released to go home.

**DESIGNATED AREA** - The geographic area designated under a Presidential major disaster declaration that is eligible to receive disaster assistance in accordance with the provisions of the Stafford Act.

**DIRECT FEDERAL ASSISTANCE** - Is provided to the affected State and local jurisdictions when they lack the resources to provide specific types of disaster assistance either because of the specialized nature of the assistance, or because of resource shortfalls (e.g., providing debris removal, potable water, emergency medical services, urban search and rescue).

**DIAL BACKUP** - The use of dial-up communication lines as a backup to dedicated lines.

**DISASTER** - Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time.

**DISASTER MANAGEMENT** - The function of controlling activities of an organization that are taken in response to a disaster situation. The functions of a management team in an operating center are functions of disaster management. Disaster management continues through the recovery stages until normal business function resumes.

**DISASTER MEDICAL ASSISTANCE TEAM** - The basic deployable unit of the NDMS, which is administered by the DHS. Staffed with physicians, nurses, other healthcare professionals, and support staff, DMAT capabilities include triage and stabilization of patients at a disaster site and provision of austere medical services at transfer points during transport to definitive medical care locations.

**DISASTER PREVENTION - MEASURES** employed to prevent, detect, or contain incidents which, if unchecked, could result in disaster.

**DISASTER PREVENTION CHECKLIST** - A questionnaire used to assess preventative measures in areas of operations such as overall security, software, data files, data entry reports, microcomputers, and personnel.

**DISASTER RECOVERY** - The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.

**DISASTER RECOVERY ADMINISTRATOR** - The individual responsible for documenting recovery activities and tracking recovery progress.

**DISASTER RECOVERY COORDINATOR** - The disaster recovery coordinator may be responsible for overall recovery of an organization or unit(s).

**DISASTER RECOVERY PERIOD** - The time period between a disaster occurrence and return to normal functions during which the disaster recovery plan is employed.

## PHASE II

### Glossary continued

---

**DISASTER RECOVERY PLAN** - The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

**DISASTER RECOVERY PLANNING** - The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster.

**DISASTER RECOVERY LIFE CYCLE** - Consists of (1) Normal Operations—the period of time before a disaster occurs; (2) Emergency Response—the hours or days immediately following a disaster; (3) Interim Processing—the period of time from the occurrence of a disaster until temporary operations are restored; and, (4) Restoration—the time when operations return to normal.

**DOMESTIC EMERGENCY SUPPORT TEAM** - PDD-39 defines the DEST as a rapidly deployable interagency support team established to ensure the full range of necessary expertise and capabilities are available to the on-scene coordinator. DHS is responsible for the DEST in domestic incidents.

**DOWNLOADING** - Connecting to another computer and retrieving a copy of a program or file from that computer.

**DUE DILIGENCE** - The practice of gathering the necessary information on actual or potential risks so that a well formulated decision may be reached regarding the potential for financial loss.

**DUTY OFFICER** - A 24-hour position within the Department of Public Safety Communications Center and also within the Division of Emergency Management. The duty officer is the statewide point of contact for alerting state agencies of emergencies/ disasters.

**EMERGENCY** - A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

**EMERGENCY FUNCTIONS** - Includes warning and communications services, relocation of persons from stricken areas, radiological preparedness, temporary restoration of utilities, plant protection, transportation, welfare, engineering, search, rescue, health, law enforcement, fire fighting and other activities.

**EMERGENCY MANAGEMENT** - The discipline which ensures an agency's, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner. Emergency management includes the preparation for, response to, recovery from and mitigation against any disaster.

**EMERGENCY PREPAREDNESS** - The part of the overall contingency plan or related activities that occurs prior to the disaster or event and is focused on the safety of personnel and the protection of critical assets. The contingency plan may reference the emergency preparedness program of the safety office or some other responsible organization.

**EMERGENCY PROCEDURES** - A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.

## PHASE II

### Glossary continued

---

**EMERGENCY RESPONSE PLANNING** - The portion of contingency planning that is focused on the immediate aftermath of a disaster or event. Emergency response planning includes the activities required to stabilize a situation and to protect lives and property.

**EMERGENCY RESPONSE UNIT-DEPARTMENT OF ENVIRONMENTAL QUALITY** -A group of occupational specialists who act as the SOSC for non-transportation hazardous materials incidents to provide scientific support and technical response activities.

**EVENT** - An occurrence that elicits a response. An unexpected event is an exception to the rule and poses a condition or set of conditions which can escalate in severity if an appropriate and timely response does not take place. For the contingency planner, a disaster, interruption, or any other occurrence, which causes the contingency plan to be activated, or considered for activation.

**EXECUTIVE SUCCESSION** - That part of the contingency plan which defines the order in which agency executives will assume operational control of the agency in the absence of the primary agency head.

**EXERCISE** - A test or drill in which actions in the contingency plan are performed or simulated as though responding to an event. It is during the exercise that planners and participants can evaluate whether the planned activities and tasks properly address potential situations.

**EXPOSURE** - A state of condition of being unprotected or vulnerable to harm or loss. In the business sense, exposure is the condition of having agency assets and/or resources subject to risk.

**EXTENDED OUTAGE** - A lengthy, unplanned interruption in system availability due to computer hardware or software problems or communication failures.

**EXERCISE** - The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

**FACILITY** - All buildings, equipment, structures, and other stationary items which are located on a single site or on contiguous or adjacent sites and which are owned or operated by the same person.

**FACILITY EMERGENCY COORDINATOR** - Facility representative for each facility with an extremely hazardous substance in a quantity exceeding its threshold planning quantity, who participates in the emergency planning process.

**FEDERAL-STATE AGREEMENT** - Once the President has declared an Emergency or a Major Disaster, the Federal Coordinating Officer and the State Coordinating Officer establish the Federal-State Agreement, which delineates the responsibilities of each party to the recovery from the disaster/emergency.

**FILE BACKUP** - The practice of dumping (copying) a file stored on disk or tape to another disk or tape. This is done for protection case the active file gets damaged.

**FILE RECOVERY** - The restoration of computer files using backup copies.



## PHASE II

### Glossary continued

---

**FINANCIAL IMPACT** - An operating expense that continues following an interruption or disaster, which, as a result of the event, cannot be offset by income and directly affects the financial position of the organization.

**FORWARD RECOVERY** - The process of recovering a data base to the point of failure by applying active journal or log data to the current backup files of the data base.

**FULL RECOVERY TEST** - An exercise in which all recovery procedures and strategies are tested (as opposed to a partial recovery test.)

**GENERATOR** - An independent source of power usually fueled by diesel or natural gas.

**HALON** - A gas used to extinguish fires effective only in closed areas.

**HAZARD** - A dangerous situation or event which may or may not lead to an emergency or a disaster.

**HAZARDOUS MATERIAL** - A term used in this plan to generically define any chemical, substance, material or waste which may pose an unreasonable risk to health, safety, property and/or the environment.

**HAZARDOUS MATERIAL (USDOT)** - Any substance which has been determined by the U. S. Department of Transportation under Title 49 CFR to be capable of posing an unreasonable risk to health, safety and property if transported in commerce.

**HAZARDOUS MATERIAL TEAM (HAZMAT)** - A team of professionals trained in handling, storage and disposal of hazardous material.

**HAZARDOUS MATERIALS UNIT - DEPARTMENT OF PUBLIC SAFETY** - A group of hazardous materials technicians and specialists who act as the SOSOC for hazardous materials highway and rail transportation incidents.

**HAZARDOUS SUBSTANCE** -A substance designated as hazardous under the Comprehensive Environmental Response Compensation and Liability Act of 1980 (CERCLA) Public Law 96-510 as amended by SARA.

**HAZARDOUS WASTE** - Has the meaning as defined in PL 94-580, Resource Conservation and Recovery Act of 1976 as amended.

**INCIDENT ACTION PLAN** - A verbal or written plan reflecting FCO/State Coordinating Officer (SCO) priorities with tactical objectives for the next operational period.

**INCIDENT COMMAND SYSTEM (ICS)** - An on-site incident management system applicable to all types of emergencies. Includes standard organizational structure, agency qualifications, training requirements, procedures, and terminology enabling participating agencies to function together effectively and efficiently.

**INCIDENT COMMANDER (IC)** - The lead agency representative in overall command of an emergency incident.



## PHASE II

### Glossary continued

---

**HAZARDOUS MATERIAL TEAM (HAZMAT)** - A team of professionals trained in handling, storage and disposal of hazardous material.

**INTERAGENCY CONTINGENCY PLANNING REGULATION** - A regulation written and imposed by the Federal Financial Institutions Examination Council concerning the need for financial institutions to maintain a working disaster recovery plan.

**INTERIM PROCESSING PERIOD** - The period of time between the occurrence of a disaster and time when normal operations are restored.

**INVENTORY FORMS** - Emergency and hazardous chemical inventory forms used for reporting under SARA Title III.

**LOCAL AREA NETWORK (LAN)** - Computing equipment, in close proximity to each other, connected to a server which houses software that can be access by the users. This method does not utilize a public carrier. See also Wide Area Network (WAN).

**LOCAL DISTRIBUTION CENTER** - A local church, community-based organization facility or site, voluntary agency facility or local government facility where goods are dispersed directly to disaster victims. Managed locally and re-supplied by parent organizations or direct supply from unexpected donors.

**LOCAL EMERGENCY** - Means the existence of conditions of disaster or extreme peril to the safety of persons or property within the territorial limits of a county, city or town, which are or are likely to be beyond the control of the services, personnel, equipment and facilities of such political subdivision as determined by its governing body and which require the combined efforts of other political subdivisions.

**LOCAL EMERGENCY PLANNING COMMITTEE (LEPC)** - A committee formed to implement local government compliance with SARA Title III. This committee is responsible for the development and maintenance of the local hazardous materials plan, and providing community right-to-know information.

**LOCAL INCIDENT COMMANDER** - The local government representative at an incident who is responsible for the direction and coordination of all local government response activities on scene.

**LOSS** - The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

**LOSS REDUCTION** - The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of loss reduction include sprinkler systems, insurance policies, and evacuation procedures.

**MATERIAL SAFETY DATA SHEETS (MSDS)** - Technical information documents required under the OSHA Hazard Communications Standard describing the toxicity, physical hazards and methods of safe handling for hazardous chemicals.

## PHASE II

### Glossary continued

---

**MEMORANDUM OF AGREEMENT/UNDERSTANDING (MOA/MOU)** - Written agreement between a sponsoring organization and other State/Local jurisdictions of the sponsoring organization. The MOA outlines responsibilities of each signatory in the event of an activation of the agreement/understanding. The MOA/MOU serves as the basis for reimbursement of task force operational expenditures during activation.

**MISSION** - In a government environment, the mission is the organization's reason for existing.

**MITIGATION** - Any measure taken to reduce or eliminate the exposure of assets or resources to long-term risk caused by natural, human caused or technological hazards. Any measures taken to reduce frequency, magnitude, and intensity of exposure to risk or to minimize the potential impact of a threat.

**MOBILIZATION** - The activation of the recovery organization in response to an emergency or disaster declaration.

**NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS)** - National structure of organization of facilities, equipment, personnel, procedures, and communications with responsibility for management of assigned resources to effectively direct and control incident responses. Can expand or contract as situation warrants with requiring a different command structure.

**NATURAL THREATS** - Events caused by nature causing disruptions to an organization.

**NETWORK ARCHITECTURE** - The basic layout of a computer and its attached systems, such as terminals and the paths between them.

**NETWORK OUTAGE** - An interruption in system availability as a result of a communication failure affecting a network of computer terminals, processors, or workstations.

**NODE** - The name used to designate a part of a network. This may be used to describe one of the links in the network, or a type of link in the network (for example, host node or intercept node).

**NONESSENTIAL RECORDS** - Records or documents which, if irretrievably lost or damaged, will not materially impair the organization's ability to conduct business.

**NOTIFICATION LIST** - A list of key individuals to be contacted, usually in the event of a disaster. Notification lists normally contain phone numbers and addresses, which may be used in the event that telephones are not operational.

**NUCLEAR WEAPONS** - The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

**OCCUPATIONAL HEALTH AND SAFETY ADMINISTRATION (OSHA)** - Regulates occupational exposures to hazardous chemicals.

**OFF-LINE PROCESSING** - A backup mode of operation in which processing can continue manually or in batch mode if the on-line systems are unavailable.

## PHASE II

### Glossary continued

---

**OFF-SITE STORAGE FACILITY** - A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.

**ON-LINE SYSTEMS** - An interactive computer system supporting users over a network of computer terminals.

**OPERATING SOFTWARE** - A type of system software supervising and directing all of the other software components plus the computer hardware.

**OPERATIONS CENTER** - A facility established for the direction of resources and coordination of response and recovery activities.

**ORGANIZATION CHART** - A diagram representative of the hierarchy of an organization's personnel.

**ORGANIZATION-WIDE** - A policy or function applicable to the entire organization and not just one single department.

**OUTSOURCING** - The transfer of data processing functions to an independent third party.

**PARALLEL TEST** - A test of recovery procedures in which the objective is to parallel an actual business cycle.

**PERIPHERAL EQUIPMENT** - Devices connected to a computer processor which perform such auxiliary functions as communications, data storage, printing, etc.

**PHYSICAL SAFEGUARDS** - Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.

**PLATFORM** - A hardware or software architecture of a particular model or family of computers (i.e., IBM, Tandem, HP, etc.)

**PLAN MAINTENANCE** - Periodic and regular review and updating of a contingency plan.

**PLANNING SOFTWARE** - A computer program designed to assist in the development, organization, printing, distribution, and maintenance of contingency plans.

**POINT OF ARRIVAL (POA)** - The designated location (typically an airport) within or near the disaster-affected area where newly arriving staff, equipment, and supplies are initially directed. Upon arrival, personnel and other resources are dispatched to either the DFO, a mobilization center, a staging area, or directly to a disaster site.

**PORTABLE SHELL** - An environmentally protected and readied structure that can be transported to a disaster site so equipment can be obtained and installed near the original location

**PREPAREDNESS** - The development of plans and procedures by government, organizations and individuals to save lives and minimize disaster damage and enhance disaster response operations.

**PROCEDURAL SAFEGUARDS** - Procedural measures taken to prevent a disaster, such as safety inspections, fire drills, security awareness programs, records retention programs, etc.

## PHASE II

### Glossary continued

---

**PROCESSING BACKLOG** - The documentation of work and processes that were performed by manual or other means during the time that the data center was unavailable.

**RECEPTION CENTER** - A large facility away from the disaster area to serve as a holding station for un-designated goods managed by State and AzVOAD representatives.

**RECIPROCAL AGREEMENT** - A mutual aid agreement between two departments, divisions, or agencies wherein each agrees to provide backup data processing support to the other in the event of a disaster. These require a substantial degree of hardware and software compatibility between the supporting and supported partners. The supporting partners must have the excess capacity to accommodate the sending partner's most critical applications.

**RECORD RETENTION** - Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.

**RECOVERY** - Activities traditionally associated with providing supplemental disaster relief assistance under a major disaster declaration. These activities usually begin within days after the event and continue after response activity ceases. Recovery includes individual and public assistance programs that provide temporary housing assistance, as well as grants and loans to eligible individuals and government entities to recover from the effects of a disaster.

**RECOVERY ACTION PLAN** - The comprehensive set of documented tasks to be carried out during recovery operations.

**RECOVERY CAPABILITY** - This defines all of the components necessary to perform recovery. These components can include a plan, an alternate site, change control process, network rerouting and others.

**RECOVERY PLANNING** - Team: A group of individuals appointed to oversee the development and implementation of a disaster recovery plan.

**RECOVERY POINT OBJECTIVE (RPO)** - The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

**RECOVERY STRATEGY** - The method selected by an organization to recover its critical business functions following a disaster. Possible strategies for recovering from an event which degrades or halts scheduled data processing services delivery are: 1. Revert to manual procedures. 2. Temporarily suspend data processing operations to effect recovery on-site. 3. Contract with a service to provide essential data processing operations from that location. 4. Transfer essential data files and applications from off-site storage to a hot-site facility and begin processing from the hot site.

**RECOVERY TIME** - The period from the disaster declaration to the recovery of critical functions.

**REDUNDANCY** - Providing two or more resources to support a single function or activity with the intention that if one resource fails or is interrupted, an alternate resource will immediately begin to perform the function

## PHASE II

### Glossary continued

---

**RESPONSE** - Activities to address the immediate and short-term effects of an emergency or disaster. Response includes immediate actions to save lives, protect property, and meet basic human needs. Based on the requirements of the situation, response assistance will be provided to an affected State under the FRP using a partial activation of selected ESFs or the full activation of all ESFs to meet the needs of the situation.

**RESOURCE CONSERVATION AND RECOVERY ACT OF 1976 (RCRA)** - Establishes a framework for proper management and disposal of all wastes.

**RESPONSE** - Means activities that are designed to provide emergency assistance, limit the primary effects, reduce the probability of secondary damage and speed recovery operations.

**RESTORATION** - The act of returning a piece of equipment or some other resource, to operational status. Commercial service companies provide a restoration service with staff skilled in restoring sensitive equipment or large facilities.

**RESUMPTION** - The process of planning for and/or implementing the recovery of critical business operations immediately following an interruption or disaster.

**RISK** - The potential for harm or loss. The chance that an undesirable event will occur.

**RISK ANALYSIS/ASSESSMENT** - The process of identifying and minimizing the exposures to certain threats which a organization may experience.

**Salvage and Restoration:** The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc., following a disaster.

**SALVAGE PROCEDURES** - Specified procedures to be activated if equipment or a facility should suffer any destruction.

**SARA** - See Superfund Amendments and Reauthorization Act of 1986

**SCENARIO** - A predefined set of events and conditions which describe an interruption, disruption or disaster related to some aspect(s) of an organization's business for purposes of exercising a recovery plan(s). Scenarios are used in developing exercises.

**SECONDARY DISASTERS** - Disasters which occur as collateral events associated with a primary disaster. Earthquakes are primary disasters which may cause subsequent fires, after shocks etc.

**SINGLE POINT OF FAILURE** - An element of a system for which no redundancy exists. A failure of such a component may disable the entire system.

**SKILLS INVENTORY** - A roster of employees that lists their skills that apply to recovery.

**SPILL** - Includes, but is not limited to, any spilling, leaking, pumping, pouring, emitting, emptying, or dumping of any hazardous material or oil.

**STAND-ALONE PROCESSING** - Processing, typically on a PC or mid-range computer, which does not require any communication link with a mainframe or other processor.

## PHASE II

### Glossary continued

---

**STAND DOWN** - Formal notification that the alert may be called off or that the state of disaster is over.

**STATE COORDINATING OFFICER (SCO)** - Appointed by the Governor to oversee disaster operations for the state.

**STATE OF EMERGENCY** - Means the duly proclaimed existence of disaster or of extreme peril to the safety of persons or property within the state caused by air pollution, fire, flood or flood-water, storm, epidemic, riot, earthquake or other causes, except those resulting in a state of war emergency, which are or are likely to be beyond the control of the services, personnel, equipment and facilities of any single county, city or town, and which require the combined efforts of the state and the political subdivision.

**STATE OF WAR EMERGENCY** - Means the condition that exists immediately whenever this nation is attacked or upon receipt by this state of a warning from the federal government indicating that such an attack is imminent.

**STATE ON-SCENE COORDINATOR (SOSC)** - The designated coordinator of all Arizona state response agencies at an incident.

**STATEWIDE INFRASTRUCTURE PROTECTION CENTER (SIPC)** - A technology security center managed by ADOA/ISD/SECURITY for the prevention, awareness, and reporting of cyber-crime and cyber-terrorism activities throughout state government.

**STRESS** - A response characterized by physical and psychological arousal arising as a direct result of an exposure to any demand or pressure on a living organism.

**SYSTEM OUTAGE** - An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.

**TABLE-TOP EXERCISE** - A type of test of a contingency plan in which actions are not actually performed. Participants read through the steps and procedures of the plan, in sequence, and evaluate the expected effectiveness of the plan the interaction between elements of the plan.

**TECHNICAL THREATS** - A disaster causing event that may occur regardless of any human elements.

**TEMPORARY OPERATING PROCEDURES** - Predetermined procedures which streamline operations while maintaining an acceptable level of control and auditability during a disaster situation.

**TERRORIST INCIDENT** - The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

**THREAT** - Threats are events that cause a risk to become a loss. Example: A lightning strike could be the trigger that causes a fire that destroys a facility. Threats include natural phenomena and human caused incidents.

## PHASE II

### Glossary continued

---

**TOLERANCE THRESHOLD** - The maximum period of time which an agency can afford to be without a critical function or process.

**TOXIC CHEMICAL** - Any substance on the list described in Section 313© of Title III.

**TRAUMA** - A trauma is any event that attacks the psyche and breaks through the defense system with the potential to significantly disrupt one's life, perhaps resulting in a personality change or physical illness if it is not managed quickly and/or effectively.

**TRAUMATIC STRESS** - The stress response produced when a person is exposed to a disturbing traumatic event. The traumatic stress reaction may be immediate or delayed.

**UNAFFILIATED VOLUNTEERS** - Also known as "emergent" volunteers that are not formally associated with a voluntary organization active in the disaster operation.

**UNINTERRUPTIBLE POWER SUPPLY (UPS)** - A backup power supply with enough power to allow a safe and orderly shutdown of the central processing unit should there be a disruption

**UNSOLICITED GOODS** - Donated items that have not been requested by government officials, voluntary disaster relief organizations, or other donations-related personnel.

**USER PREPAREDNESS REVIEWS** - Periodic simulations of disaster recovery conditions for the purpose of evaluating how well an individual or department is prepared to cope with disaster conditions.

**VULNERABILITY** - The degree to which people, property, resources, and commerce, as well as environmental, social, and cultural activity are susceptible to harm or destruction.

**VITAL RECORDS** - Records or documents, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization's ability to conduct business.

**WEAPON OF MASS DESTRUCTION** - Title 18, U.S.C. 2332a, defines a WMD as (1) any destructive device as defined in Section 921 of this title, [which reads] any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, mine, or device similar to the above; (2) poison gas; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.